ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

Internet of Things (IoT) και Ασφάλεια Πληροφοριακών Συστημάτων

Ιωάννης Αποστολόπουλος

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων

Γεώργιος Δημητρίου

Λαμία, 2019

UNIVERSITY OF THESSALY

SCHOOL OF SCIENCE

INFORMATICS AND COMPUTATIONAL BIOMEDICINE

«Internet of Things (IoT) and Information Systems Security»

Ioannis Apostolopoulos

Master thesis

Georgios Dimitriou

Lamia, 2019

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ
ΚΑΤΕΥΘΥΝΣΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ

Internet of Things (IoT) και Ασφάλεια Πληροφοριακών Συστημάτων

Ιωάννης Αποστολόπουλος

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων

Γεώργιος Δημητρίου

Λαμία, 2019

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο «Internet of Things (IoT) και Ασφάλεια Πληροφοριακών Συστημάτων» αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο ΔΗΛΩΝ

Ημερομηνία

Υπογραφή

Internet of Things (IoT) και Ασφάλεια Πληροφοριακών Συστημάτων

Ιωάννης Αποστολόπουλος

Τριμελής Επιτροπή:

Γεώργιος Δημητρίου

Γεώργιος Σταμούλης

Αντώνης Δαδαλιάρης

Επιστημονικός Σύμβουλος:

Γεώργιος Δημητρίου

Επιτελική Σύνοψη

Υπάρχουν δισεκατομμύρια συσκευές συνδεδεμένες συνθέτοντας το λέγόμενο Διαδίκτυο των Πραγμάτων (IoT), και συνεχώς ο αριθμός τους αυξάνεται. Ως διαρκής τεχνολογία, το Διαδίκτυο μπορεί να χρησιμοποιηθεί σε διάφορους τομείς προς όφελος της ανθρώπινης ζωής και ενασχόλησης. Το IoT αλλάζει τον κόσμο μας και τον τρόπο που ζούμε. Ωστόσο, το IoT δεν έχει ενιαία αρχιτεκτονική και εκεί είναι που παρατηρούνται διαφορετικά είδη κακόβουλων επιθέσεων στα διάφορα επίπεδα του IoT. Οι συσκευές IoT είναι πιο ευάλωτες σε επιθέσεις επειδή κάποιες από αυτές είναι απλές και δεν μπορούν να ληφθούν μέτρα ασφαλείας. Στο παρόν πόνημα αναλύονται στο 1ο Κεφάλαιο τι σημαίνει Διαδίκτυο των Πραγμάτων και ποια είναι η αρχιτεκτονική δικτύου του, ενώ στο 2ο Κεφάλαιο δίνονται στον αναγνώστη οι θεμελιώδεις έννοιες της Ασφάλειας των Πληροφοριακών Συστημάτων και οι κίνδυνοι από τα κακόβουλα προγράμματα, σε συνδυασμό με το IoT. Αναλύεται, επίσης, η ταξινόμηση των επιθέσεων στο IoT, ενώ έχει μεγάλη σημασία η ασφάλεια στο υπολογιστικό νέφος του IoT. Στο 3ο Κεφάλαιο δίνεται ένα εμπεριστατωμένο πλαίσιο πολιτικών ασφαλείας στο IoT, έτσι όπως διαμορφώνεται από την σύγχρονη βιβλιογραφία και νέους διεθνείς κανονισμούς. Συμπερασματικά, η παρούσα Διπλωματική Εργασία επιχειρεί να αποτελέσει ένα σύγχρονο State of the Art της Ασφάλειας Πληροφοριακών Συστημάτων στο IoT, καθώς οι επιστημονικές δημοσιεύσεις επί του γνωστικού θέματος τείνουν να αυξάνονται συνεχώς τα τελευταία επί του παρόντος έτη.

Ευχαριστίες

Ευχαριστώ θερμά τον καθηγητή μου κ. Δημητρίου για τις πολύτιμες συμβουλές του και την υπομονετική καθοδήγησή του.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Επιτελική Σύνοψη 7

Ευχαριστίες 8

Κεφάλαιο 1 - Εισαγωγικά στοιχεία του Διαδικτύου των Πραγμάτων (IoT) 10

1.1 Τι είναι το Internet of Things 10

1.1.1 Γενική επισκόπηση 10

1.1.2 Αρχιτεκτονική IoT 14

1.1.3 Μοντέλα συνδεσιμότητας & επικοινωνίας 16

1.2 Εφαρμογές IoT 19

Κεφάλαιο 2 - IoT και Θέματα Ασφάλειας 25

2.1 Θεμελιώδεις έννοιες Ασφάλειας Πληροφοριακών Συστημάτων 25

2.1.1 Επιθέσεις κακόβουλου λογισμικού 27

2.1.2 Η εποχή της Κυβερνο-Απειλής & Κυβερνο-ασφάλειας 31

2.2 Ιδιωτικότητα στο IoT 35

2.3 Ταξινόμηση επιθέσεων στο IoT 36

2.4 Στοιχεία Ασφάλειας στην IoT Νεφοϋπολογιστική 46

Κεφάλαιο 3 - Επισκόπηση στο σύγχρονο πλαίσιο Προστασίας του IoT 50

3.1 Προτεινόμενο πλαίσιο ασφάλειας του IoT 50

3.2 Νέος Κανονισμός GDPR: Τι σημαίνει για το IoT 56

Κεφάλαιο 4 - Συμπεράσματα 61

Βιβλιογραφικές πηγές 64

Κεφάλαιο 1

Εισαγωγικά στοιχεία του Διαδικτύου των Πραγμάτων (IoT)

1.1 Τι είναι το Internet of Things

Οι διασυνδεδεμένες τεχνολογίες είναι αυτές που εμπεριέχουν την έννοια της επικοινωνίας μεταξύ ανθρώπων αλλά και μεταξύ μηχανών. Χαρακτηριστικό όλων των Επιστημών, έτσι και της Τεχνολογίας, είναι η εξέλιξη. Επιστημονικοί, εμπορικοί, πολιτικοί και κοινωνικοί παράγοντες συνετέλεσαν και συνεχίζουν να συντελούν την συνιστώσα εξελικτική δύναμη της Τεχνολογίας και της Επιστήμης των Υπολογιστών. Είναι γενικά αποδεκτό ότι μεταπολεμικά του Β' Παγκοσμίου Πολέμου, η λαχτάρα για την κατάκτηση του διαστήματος συμπαρέσυρε υποχρεωτικά την εξέλιξη των τηλεπικοινωνιών, η οποία με την σειρά της έφερε την εφεύρεση της διαδικτυακής επικοινωνίας (βλ. Ιστορική αναδρομή Διαδικτύου). Τελικά, η ανάπτυξη του διαδικτύου σχετίζεται αμιγώς με την εξέλιξη των σύγχρονων Πληροφοριακών και Τηλεπικοινωνιακών Συστημάτων.

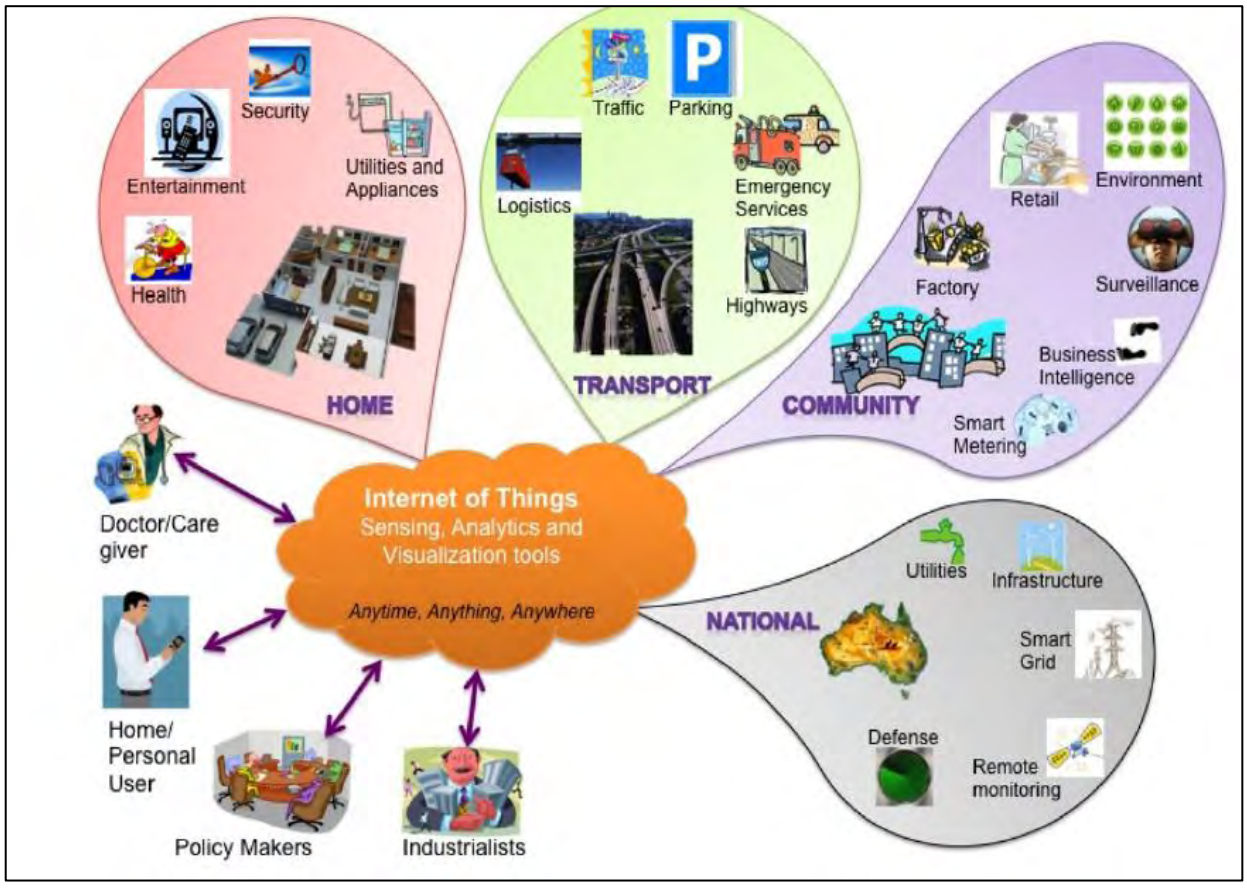
1.1.1 Γενική επισκόπηση

Το Διαδίκτυο των πραγμάτων (IoT), που ονομάζεται επίσης το Διαδίκτυο του Everything (IoE), είναι ένα νέο τεχνολογικό επίτευγμα, που έχει οραματιστεί ως το παγκόσμιο δίκτυο των υπολογιστικών μηχανών και των ηλεκτρονικών συσκευών που μπορούν να αλληλεπιδρούν με ο ένας τον άλλον. Το IoT αναγνωρίζεται ως ένας από τους πλέον σημαντικούς τομείς της σύγχρονης και μελλοντικής τεχνολογίας και κερδίζει μεγάλη προσοχή από ένα ευρύ φάσμα βιομηχανιών. Το IoT είναι μια συλλογή πολλών

διασυνδεδεμένων αντικείμενων, υπηρεσιών, ανθρώπων και συσκευών, που μπορούν να επικοινωνούν, να διαμοιράζονται δεδομένα και πληροφορίες, με σκοπό να επιτύχουν ένα κοινό στόχο σε διάφορους τομείς και εφαρμογές. Οι συσκευές του IoT ακολουθούν ένα «Identity Management» που προσδιορίζεται σε ομοιογενείς και ετερογενείς συσκευές. Ομοίως, μια περιοχή IoT μπορεί να οριστεί από μία διεύθυνση IP, αλλά κάθε συσκευή μέσα στην περιοχή αυτή μπορεί να έχει την δική της διεύθυνση IP.

Ο όρος IoT δημιουργήθηκε για πρώτη φορά από τον Kevin Ashton το 1999 στο πλαίσιο της διαχείρισης της αλυσίδας εφοδιασμού [1]. Ωστόσο, κατά την τελευταία δεκαετία, ο ορισμός έχει καλύψει περισσότερο ευρύ φάσμα εφαρμογών όπως η υγειονομική περίθαλψη, οι υπηρεσίες κοινής ωφελείας, διανομής ενέργειας, κ.λπ. [2]. Αν και ο ορισμός των «Things» άλλαξε όσο η τεχνολογία εξελίχθηκε, ο κύριος στόχος της παροχής πληροφόρησης σχετικά με τον Η/Υ χωρίς την βοήθεια της ανθρώπινης παρέμβασης παραμένει η ίδια. Μια ριζική εξέλιξη του τρέχοντος Διαδικτύου σε ένα Δίκτυο διασυνδεδεμένων αντικειμένων που όχι μόνο συλλέγει πληροφορίες από το περιβάλλον (ανίχνευση) και αλληλεπιδρά με τον φυσικό κόσμο (ενεργοποίηση / εντολή / έλεγχος), αλλά χρησιμοποιεί επίσης τα υπάρχοντα πρότυπα του Διαδικτύου να παρέχει υπηρεσίες για τη μεταφορά πληροφοριών, αναλύσεις, εφαρμογές και επικοινωνίες. Τροφοδοτείται από την επικράτηση των ενεργοποιημένων συσκευών με ανοικτή ασύρματη τεχνολογία, όπως Bluetooth, ραδιοσυχνότητα (RFID), Wi-Fi και υπηρεσίες τηλεφωνικών δεδομένων, καθώς και ενσωματωμένους κόμβους αισθητήρα και ενεργοποιητή. Η επανάσταση στο Διαδίκτυο οδήγησε στη διασύνδεση μεταξύ ανθρώπων χωρίς προηγούμενη κλίμακα και ρυθμό. Η επόμενη επανάσταση θα είναι η διασύνδεση μεταξύ αντικείμενων για να δημιουργηθεί ένα έξυπνο περιβάλλον. Από το 2011 ο αριθμός των διασυνδεδεμένων συσκευών στον πλανήτη υπερβαίνει τον αριθμό των ανθρώπων. Επί του παρόντος, υπάρχουν 9 δισεκατομμύρια διασυνδεδεμένες συσκευές και αναμένεται ο αριθμός να φτάσει τα 24 δισεκατομμύρια συσκευές έως το 2020. Σύμφωνα με την GSMA, αυτό ανέρχεται σε 1,3 τρισεκατομμύρια δολάρια ευκαιρίες εσόδων μόνο για τους φορείς εκμετάλλευσης κινητών δικτύων που

εκτείνονται κάθετα όπως η υγεία, η αυτοκινητοβιομηχανία, οι επιχειρήσεις κοινής ωφελείας και τα ηλεκτρονικά είδη ευρείας κατανάλωσης. Παρουσιάζεται μια σχηματική απεικόνιση της διασύνδεσης των αντικειμένων (Εικόνα 1), όπου οι τομείς εφαρμογής επιλέγονται με βάση την κλίμακα των επιπτώσεων των παραγόμενων δεδομένων. Οι χρήστες ξεκινούν από το άτομο σε οργανώσεις σε εθνικό επίπεδο που ασχολούνται με ευρύτατα ζητήματα [1].



Εικόνα 1. Σχηματική αναπαράσταση του Internet of Things (IoT) δείχνοντας τους τελικούς χρήστες και τα πεδία εφαρμογής.

Παρόλο που το παγκόσμιο ενδιαφέρον είναι έντονο γύρω από το IoT, υπάρχουν πολλοί ορισμοί του. Δεν υπάρχει δηλαδή ένας κοινά αποδεκτός ορισμός. Μερικοί από τους ορισμούς που δίνονται βάσει την πηγή τους είναι:

- **IEEE – 2015 [2]**: *"Ένα παγκόσμιο δίκτυο διασυνδεδεμένων αντικειμένων με μοναδική διευθυνσιοδότηση βάσει βασικών πρωτοκόλλων επικοινωνίας".*

- **Wikipedia [3]**: ***"****Το Διαδίκτυο των πραγμάτων ή Ίντερνετ των πραγμάτων (αγγλικά: Internet of things) αποτελεί το δίκτυο επικοινωνίας πληθώρας συσκευών, οικιακών συσκευών, αυτοκινήτων καθώς και κάθε αντικειμένου που ενσωματώνει ηλεκτρονικά μέσα, λογισμικό, αισθητήρες και συνδεσιμότητα σε δίκτυο ώστε να επιτρέπεται η σύνδεση και η ανταλλαγή δεδομένων. Απλούστερα, η φιλοσοφία του IoT είναι η σύνδεση όλων των ηλεκτρονικών συσκευών μεταξύ τους (τοπικό δίκτυο) ή με δυνατότητα σύνδεσης στο διαδίκτυο (παγκόσμιο ιστό).* [1] **"**

- **Tutorials Point - Simply Easy Learning** [4]: *"Το IoT (Internet of Things) είναι ένα προηγμένο σύστημα αυτοματοποίησης και ανάλυσης που εκμεταλλεύεται τη δικτύωση, την ανίχνευση, τα μεγάλα δεδομένα και την τεχνολογία τεχνητής νοημοσύνης για την παροχή ολοκληρωμένων συστημάτων για ένα προϊόν ή μια υπηρεσία. Αυτά τα συστήματα επιτρέπουν μεγαλύτερη διαφάνεια, έλεγχο και απόδοση όταν εφαρμόζονται σε οποιοδήποτε κλάδο ή σύστημα."*

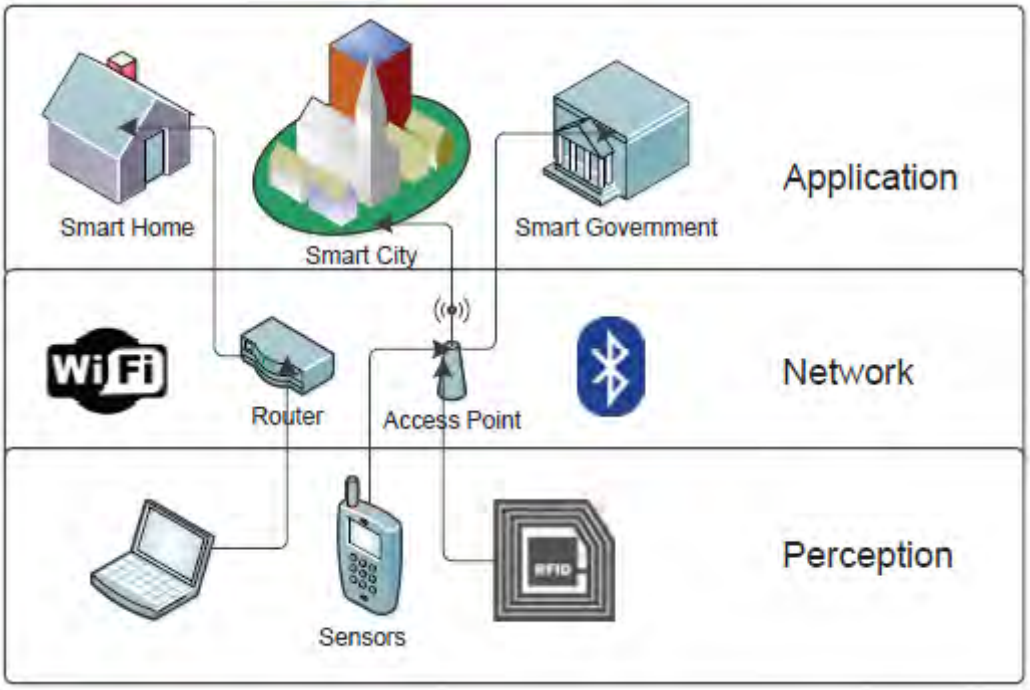
- **IEEE 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies [5]:** *"Ομάδα δομών που διασυνδέουν τα συνδεδεμένα αντικείμενα και επιτρέπουν τη διαχείρισή τους, την εξόρυξη δεδομένων και την πρόσβαση στα δεδομένα που δημιουργούν."*

1.1.2 Αρχιτεκτονική IoT

Στο IoT, κάθε επίπεδο ορίζεται από τις λειτουργίες και τις συσκευές που χρησιμοποιούνται σε αυτό. Υπάρχουν διαφορετικές απόψεις σχετικά με τον αριθμό των επιπέδων στο Διαδίκτυο. Ωστόσο, σύμφωνα με πολλούς ερευνητές, το IoT λειτουργεί σε τρία ή τέσσερα επίπεδα, όπου κάθε ένα από αυτά έχει εγγενή ζητήματα ασφάλειας που συνδέονται με το IoT [6].

3 – Layer Architecture of IoT

Η Εικόνα 2 δείχνει το βασικό αρχιτεκτονικό πλαίσιο τριών επιπέδων του IoT σε σχέση με τις συσκευές και τις τεχνολογίες που καλύπτουν κάθε επίπεδο.



Εικόνα 2. Αρχιτεκτονική 3-Layer του IoT .

Perception Layer: Το Perception Layer έχει σκοπό την απόκτηση των δεδομένων από το περιβάλλον με τη βοήθεια αισθητήρων και ενεργοποιητών. Αυτό το επίπεδο ανιχνεύει, συλλέγει και επεξεργάζεται πληροφορίες και τις μεταδίδει

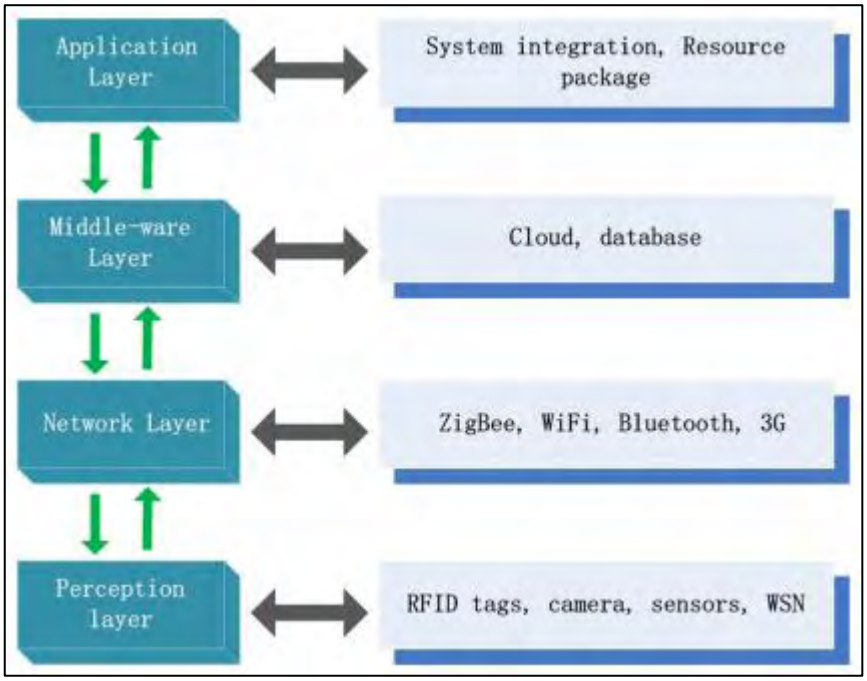
στο επίπεδο του δικτύου. Αυτή η στρώση αποτελεί επίσης τον κόμβο συνεργασίας IoT σε τοπικά δίκτυα και δίκτυα μικρής εμβέλειας [7]. Το Perception Layer περιλαμβάνει RFID αισθητήρες, κάμερες, ασύρματους αισθητήρες, κ.α. Η ασφάλεια στο επίπεδο αυτό έχει να κάνει με κακόβουλες παρεμβάσεις στους αισθητήρες και στην τεχνολογία ταυτοποίησης που παρεμβάλλονται στην συλλογή δεδομένων [8].

Network Layer: Το Network Layer εξυπηρετεί τη λειτουργία της δρομολόγησης δεδομένων και μετάδοσης σε διάφορους κόμβους και συσκευές IoT (εννοείται μέσω του Intenet). Σε αυτό το επίπεδο ανήκουν πλατφόρμες υπολογιστικού νέφους, διαδικτυακές πύλες, οι μεταγωγείς, οι συσκευές δρομολόγησης, κλπ. Λειτουργούν με τη χρήση ορισμένες από τις πολύ πρόσφατες τεχνολογίες όπως WiFi, LTE, Bluetooth, 3G/4G, κλπ. Οι πύλες δικτύου χρησιμεύουν ως μεσολαβητής μεταξύ διαφορετικών κόμβων IoT με συγκέντρωση, φιλτράρισμα, και τη μετάδοση δεδομένων από και προς διαφορετικούς αισθητήρες [9]. Οι επιθέσεις στο επίπεδο του δικτύου έχουν να κάνουν περισσότερο με την συνεργασία των συσκευών και τον διαμοιρασμό των πληροφοριών μεταξύ τους.

Application Layer: Το Application Layer (Επίπεδο Εφαρμογής) εγγυάται την αυθεντικότητα, την ακεραιότητα, και την εμπιστευτικότητα των δεδομένων. Σε αυτό το στρώμα, ο σκοπός του IoT ή η δημιουργία ενός έξυπνου περιβάλλοντος. Οι κακόβουλοι χρήστες εκμεταλλεύονται στο επίπεδο αυτό κενά ασφαλείας στον κώδικα των εφαρμογών, ώστε να αποσπάσουν ευαίσθητα δεδομένα ή να τα αλλοιώσουν.

Αρχιτεκτονική 4 επιπέδων (4 – Layer) του IoT

Νεότεροι επιστήμονες πληροφορικής, υποστηρίζουν την τετραμερή στρωμάτωση του IoT, η οποία διαφέρει στην προσθήκη του Middleware Layer, και περιγράφεται παρακάτω [10]:



Εικόνα 3. Αρχιτεκτονική 4 - Layer του IoT.

Middleware Layer: Στο επίπεδο αυτό μεταβιβάζεται πληροφορία από το επίπεδο δικτύου. Ενώνει το όλο σύστημα στο cloud και στις βάσεις δεδομένων, και διαχειρίζεται και αποθηκεύει δεδομένα. Το επίπεδο αυτό αναφέρεται κυρίως στην νεφοϋπολογιστική του IoT, προάγωντας APIs που είναι απαραίτητα στο επίπεδο εφαρμογής. Στο Middleware Layer είναι σημαντική η ασφάλεια των βάσεων δεδομένων και η ασφάλεια του νέφους, γιατί ουσιαστικά επηρεάζεται άμεσα το επίπεδο της εφαρμογής.

1.1.3 Μοντέλα συνδεσιμότητας & επικοινωνίας

Τα τρία κύρια μέρη ενός Διαδικτύου των Πραγμάτων (IoT) είναι:

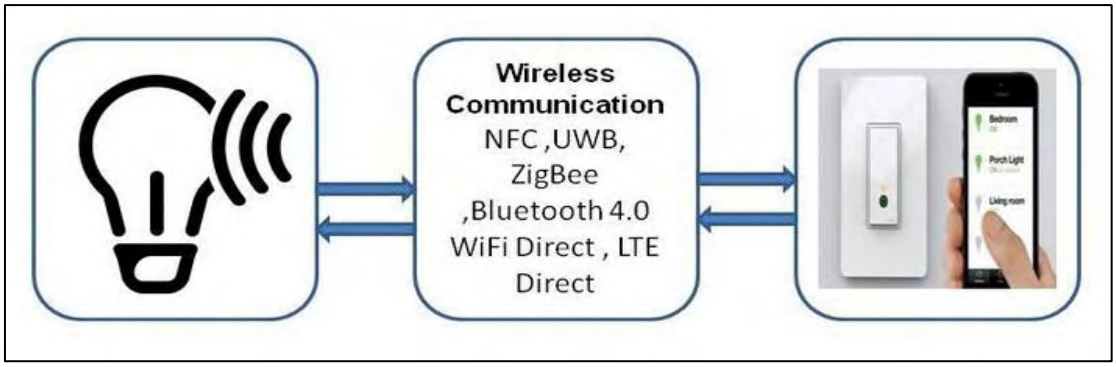
1. Τα «πράγματα» που συλλέγουν πληροφορίες οπουδήποτε και οποιαδήποτε στιγμή χρησιμοποιώντας RFID τεχνολογία, αισθητήρες και κώδικα.

2. Τα δίκτυα επικοινωνιών που συνδέουν τα «πράγματα».

3. Τα υπολογιστικά συστήματα και οι εφαρμογές που επεξεργάζονται όσα δεδομένα ρέουν από και προς τα «πράγματα» όπως το cloud computing.

Η συνδεσιμότητα των τριών αυτών μερών του IoT πραγματοποιείται με τέσσερις τρόπους δικτύωσης (σύνδεσης και επικοινωνίας) όπως περιγράφονται σε έγγραφο του Internet Architecture Board - IAB (RFC 7452, Μάρτιος 2015 - *https://tools.ietf.org/html/rfc7452*) [11] :

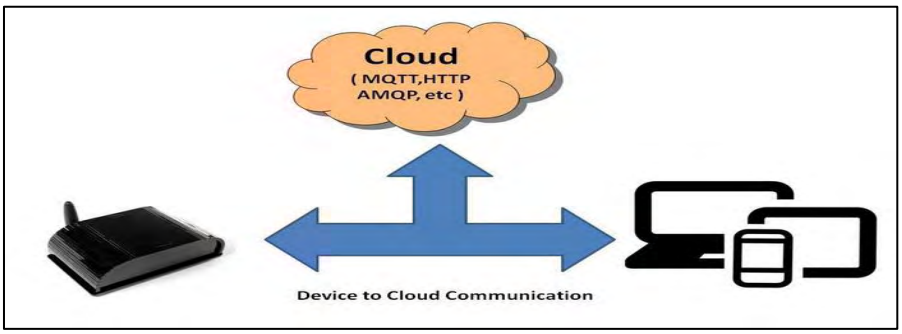
1. Device -to- Device Communication: Το μοντέλο αυτό επικοινωνίας της συσκευής προς συσκευή αντιπροσωπεύεται από δύο ή περισσότερες συσκευές που συνδέονται άμεσα και επικοινωνούν μεταξύ τους χωρίς ενδιάμεσο server. Αυτές οι συσκευές συνδέονται με πολλούς τύπους δικτύων, συμπεριλαμβανομένων των δικτύων IP ή το Internet, χρησιμοποιώντας πρωτόκολλα όπως το Bluetooth, Z-Wave, ή ZigBee (Εικόνα 4).



Εικόνα 4. Device -to -Device Communication.

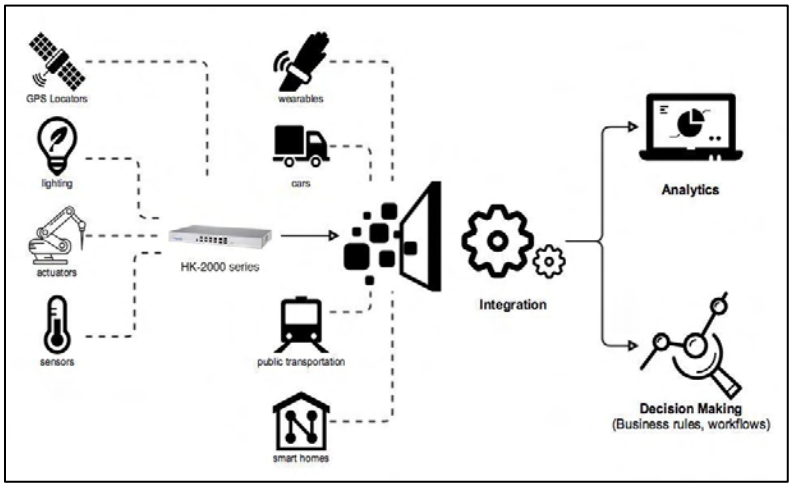
2. Device -to- Cloud Communication: Στο μοντέλο αυτό επικοινωνίας, η συσκευή IoT συνδέεται απευθείας με μια υπηρεσία cloud Internet, όπως ένας πάροχος υπηρεσιών εφαρμογών, για την ανταλλαγή δεδομένων και την κυκλοφορία μηνυμάτων ελέγχου. Αυτή η προσέγγιση εκμεταλλεύεται συχνά τους υφιστάμενους μηχανισμούς επικοινωνίας όπως οι παραδοσιακές ενσύρματες συνδέσεις Ethernet ή Wi-Fi για να δημιουργήσει μια σύνδεση μεταξύ της

συσκευής και του δικτύου IP, η οποία τελικά συνδέεται με την υπηρεσία cloud (Εικόνα 5).



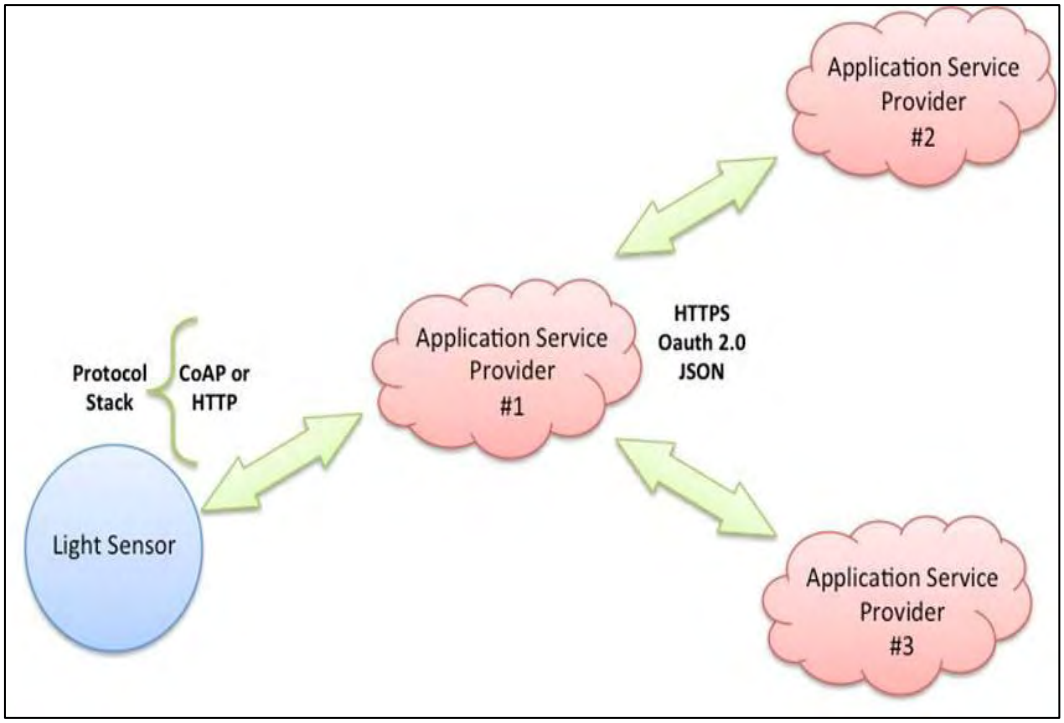
Εικόνα 5. Device -to- Cloud Communication.

3. Device -to- Gateway Model: Στο μοντέλο Device-to-Gateway, οι συσκευές IoT βασικά συνδέονται με μια ενδιάμεση συσκευή για πρόσβαση σε μια υπηρεσία σύννεφο. Αυτό το μοντέλο συχνά περιλαμβάνει λογισμικό εφαρμογών που λειτουργεί σε μια τοπική συσκευή πύλης (όπως ένα smartphone ή ένα "hub") που λειτουργεί ως ενδιάμεσος ανάμεσα σε μια συσκευή IoT και μια υπηρεσία cloud (Εικόνα 6).



Εικόνα 6. Device -to- Gateway Model

4. Backend Data Sharing: Η ανταλλαγή δεδομένων από πίσω μέρος βασικά επεκτείνει το μοντέλο ενιαίας επικοινωνίας συσκευής σε σύννεφο, έτσι ώστε οι συσκευές IoT και τα δεδομένα αισθητήρων να έχουν πρόσβαση σε εξουσιοδοτημένα τρίτα μέρη. Σύμφωνα με αυτό το μοντέλο, οι χρήστες μπορούν να εξάγουν και να αναλύουν δεδομένα έξυπνων αντικειμένων από μια υπηρεσία σύννεφο σε συνδυασμό με δεδομένα από άλλες πηγές και να τα στέλνουν σε άλλες υπηρεσίες για συνάθροιση και ανάλυση [12] (Εικόνα 7).

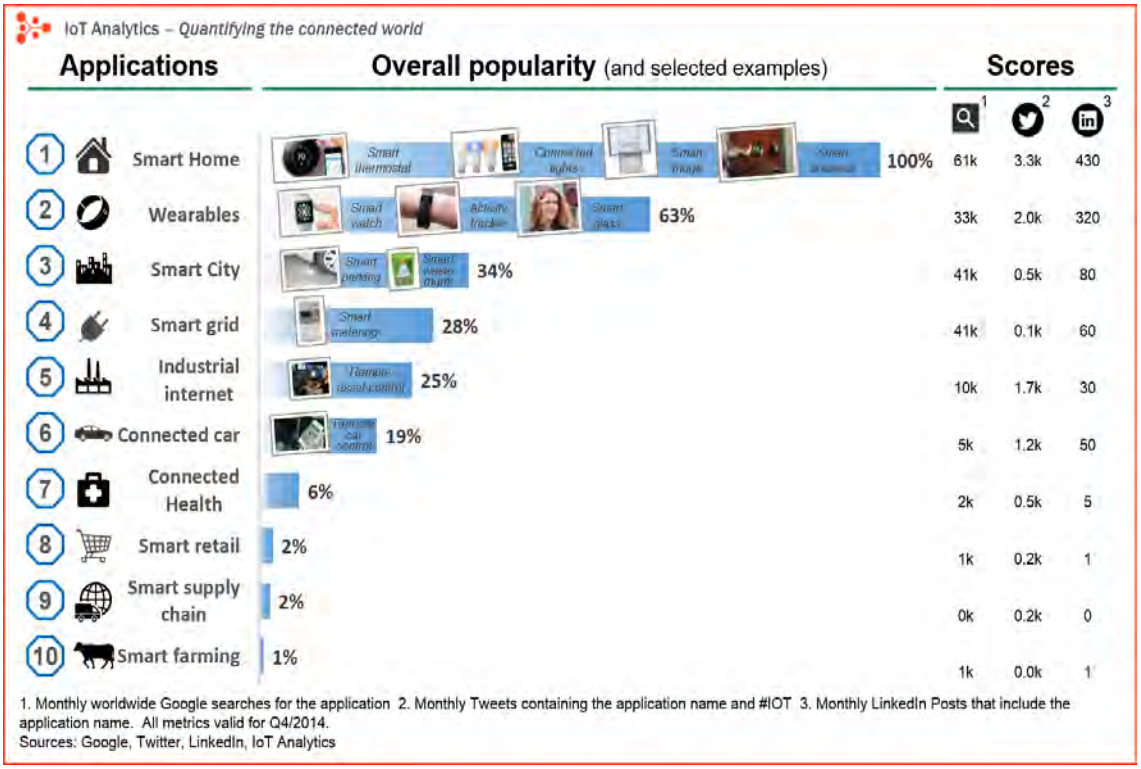


Εικόνα 7. Backend Data Sharing

1.2 Εφαρμογές IoT

Οι τεχνολογίες διαδικτύου αναμένεται να ενθαρρύνουν την καινοτομία σε ορισμένους βασικούς βιομηχανικούς τομείς, όπως της υγείας, της αυτοματοποίησης του εργοστασίου / της έξυπνης κατασκευής, της παραγωγής και διανομής τροφίμων,

της παρακολούθησης του περιβάλλοντος, των κτηρίων, του περιβάλλοντος διαβίωσης, της ενέργειας, των έξυπνων – φορητών συσκευών, των έξυπνων πόλεων, κ.λπ. [13] (Εικόνα 8).



Εικόνα 8. IoT Analytics

Αναλυτικότερα, θα μπορούσε να αναλυθεί η εφαρμογστική αξία του IoT σε μερικούς τομείς, ως φαίνεται ακολούθως [14]:

- **Στην Υγεία**

Η εμφάνιση των εφαρμογών του Διαδικτύου της Υγείας (Internet of Health - IoH) αφιερωμένη στην υγεία και την ευεξία των πολιτών που καλύπτει τη φροντίδα, την παρακολούθηση, τη διάγνωση, τη διαχείριση φαρμάκων, την καταλληλότητα κ.λπ. θα επιτρέψει στους πολίτες να εμπλακούν περισσότερο στην υγειονομική τους

περίθαλψη. Οι τελικοί χρήστες θα μπορούσαν να έχουν πρόσβαση σε ιατρικά αρχεία, να παρακολουθούν τα ζωτικά σήματα με φορητές συσκευές, να διενεργούν διαγνωστικούς εργαστηριακούς ελέγχους στο σπίτι ή στο κτίριο γραφείων και να παρακολουθούν τις συνήθειες που σχετίζονται με την υγεία με εφαρμογές που βασίζονται στο Web σε έξυπνες κινητές συσκευές. Η εφαρμογή του IoT στην υγειονομική περίθαλψη μπορεί να βελτιώσει την πρόσβαση των ατόμων σε απομακρυσμένες περιοχές ή σε άτομα που δεν μπορούν να κάνουν συχνές επισκέψεις στο νοσοκομείο. Μπορεί επίσης να επιτρέψει την έγκαιρη διάγνωση των ιατρικών καταστάσεων μέσω της μέτρησης και της ανάλυσης των παραμέτρων ενός ατόμου. Η ιατρική θεραπεία που χορηγείται στον υπό θεραπεία φροντίδα μπορεί να βελτιωθεί μελετώντας την επίδραση μιας θεραπείας και του φαρμάκου στις ζωτικές συνθήκες των ασθενών.

Οι εφαρμογές του IoT στην ιατροφαρμακευτική περίθαλψη απαιτούν μια προσεκτική ισορροπία μεταξύ της πρόσβασης σε δεδομένα και της ανταλλαγής πληροφοριών για την υγεία, σε σχέση με θέματα ασφάλειας και προστασίας της ιδιωτικής ζωής. Για αυτές τις εφαρμογές, υπάρχει ανάγκη να μεταβληθεί η ιδέα της ανθρώπινης συμπεριφοράς, ώστε οι ασθενείς να εξελιχθούν, να προσαρμοστούν και τελικά να αγκαλιάσουν την τεχνολογία του IoT που μπορεί να προσφέρει, ένα ασφαλές διαδικτυακό χώρο που μπορεί να φιλοξενήσει όλες τις υπηρεσίες υγείας.

- **Στο περιβάλλον διαβίωσης**

Το IoT μπορεί να αποφέρει οφέλη στα καθημερινά περιβάλλοντα διαβίωσης των ανθρώπων.. Οι πολίτες εργάζονται και ξοδεύουν πολλές ώρες της ημέρας σε αυτά τα περιβάλλοντα, π.χ. σπίτι, εργασία, αθλητικούς χώρους, ψυχαγωγίας, κοινωνικών δραστηριοτήτων, κλπ.. Οι άνθρωποι ασκούν και ασχολούνται με μια ευρεία ποικιλία δραστηριοτήτων που μπορούν να σχεδιαστούν για δραστηριότητες όπως οι εμπειρίες υγείας και φυσικής κατάστασης, οι εργασιακές εμπειρίες από το σπίτι και οι εμπειρίες από την κατανάλωση ενέργειας.

- **Στις κτηριακές υποδομές και διαχειρίσεις**

Οι εφαρμογές IoT στα κτήρια αλληλεπιδρούν με τα έξυπνα συστήματα διαχείρισης κτηρίων (Building Management System - BMS) που είναι επικάλυψη ενός δικτύου IP, συνδέοντας όλες τις υπηρεσίες κτιρίου παρακολούθησης, ανάλυσης και τον έλεγχο, χωρίς την παρέμβαση των ανθρώπων. Οι εφαρμογές του Διαδικτύου χρησιμοποιούνται από τους διαχειριστές κτηρίων για την διαχείριση της χρήσης ενέργειας και την προμήθεια ενέργειας, καθώς και την διατήρηση – συντήρηση συστημάτων κτηρίων. Το BMS βασίζεται στην υποδομή των υφιστάμενων Intranets και του Διαδικτύου και ως εκ τούτου χρησιμοποιεί τα ίδια πρότυπα με αυτά όπως οι άλλες συσκευές πληροφορικής. Η αξία στην εφαρμογή IoT είναι τόσο στα δεδομένα όσο και στις συσκευές ακμής. Η συλλογή δεδομένων από περισσότερες υπηρεσίες κτηρίων και εξοπλισμού παρέχει μια πιο λεπτομερή εικόνα του πώς ακριβώς κάθε κτήριο εκτελεί. Αυτά θα δημιουργήσουν τις εφαρμογές Internet του Κτιρίου (Internet of Building - IoB). Αυτές οι εφαρμογές IoT μειώνουν την ανάγκη για ανθρώπινη παρέμβαση διαχείρισης της πολυπλοκότητας. Το IoB απαιτεί τη διαλειτουργικότητα και την απρόσκοπτη ανταλλαγή δεδομένων μεταξύ διαφόρων υποσυστημάτων ενός κτηρίου, μεταξύ δικτύων κτηρίων, μεταξύ διάφορων έξυπνων συσκευών, μεταξύ εξωτερικών υπηρεσιών κοινής ωφέλειας (π.χ. έξυπνα δίκτυα, έξυπνες πόλεις κλπ.) ή με άλλους ενδιαφερόμενους φορείς.

- **Στον Ενεργειακό τομέα**

Το IoT επιτρέπει τη σύνδεση και την παρακολούθηση των ενεργειακών πόρων και αγαθών, από σχεδόν οπουδήποτε, με τη χρήση των διασυνδεδεμένων συσκευών και των επιχειρήσεων κοινής ωφέλειας και των καταναλωτών / προωθητών ενέργειας, οι οποίοι μπορούν να έχουν πρόσβαση για την παρακολούθηση και την βελτίωση της ενεργειακής απόδοσης. Χρησιμοποιώντας την τεχνολογία IoT, τα βοηθητικά προγράμματα είναι εξοπλισμένα για να παρέχουν περισσότερη ισχύ να βελτιώσουν αποτελεσματικά τις λειτουργίες, να μειώσουν τις εκπομπές και το κόστος διαχείρισης και να αποκαταστήσουν την ισχύ τους ταχύτερα, ενώ οι ενεργειακοί φορείς

εκμετάλλευσης (ιδιωτικοί και κρατικοί φορείς) είναι σε θέση να αναγνωρίσουν αμέσως τις διακοπές λειτουργίας, επιτρέποντας τη βελτίωση της αποτελεσματικότητάς τους.

- **Στην Γεωργία και Διατροφή**

Η τεχνολογία IoT επιτρέπει την παρακολούθηση και τον έλεγχο των φυτών και των ζωικών προϊόντων καθ 'όλη τη διάρκεια του κύκλου από το αγρόκτημα στο πιάτο. Η πρόκληση θα είναι στο μέλλον να σχεδιάζονται αρχιτεκτονικές και να υλοποιούνται αλγόριθμοι που θα υποστηρίζουν κάθε αντικείμενο για βέλτιστη συμπεριφορά, σύμφωνα με το ρόλο του στην έξυπνη γεωργία και στην έξυπνη τροφική αλυσίδα, μειώνοντας το οικολογικό αποτύπωμα και το οικονομικό κόστος και αυξάνοντας τα τρόφιμα και την ασφάλεια της παραγωγής και κατανάλωσης.

- **Έξυπνες φορητές συσκευές (Wearables)**

Τα προϊόντα Wearables ενσωματώνουν βασικές τεχνολογίες (π.χ. νανοηλεκτρονική, οργανικά ηλεκτρονικά, αισθητήρες, ενεργοποίηση, επικοινωνία, υπολογισμός χαμηλής ισχύος, οπτικοποίηση και ενσωματωμένο λογισμικό) σε έξυπνα συστήματα, φέροντας νέες λειτουργίες σε ρούχα, υφάσματα, ρολόγια, αξεσουάρ, και άλλες συσκευές που είναι τοποθετημένες πάνω στο σώμα. Τα τελευταία χρόνια η έρευνα της τηλεϊατρικής χρησιμοποιεί πολλά πλεονεκτήματα των Wearable συσκευών για την λήψη, διατήρηση, σύγκριση και μετάδοση πληροφορίας στην ατομική υγεία.

- **Έξυπνη πόλη (Smart City)**

Υπάρχουν ορισμένα βασικά στοιχεία που χρειάζονται για να διαμορφωθεί μια έξυπνη πόλη, και μερικά από αυτά είναι η έξυπνη κοινωνία, τα έξυπνα κτίρια, h έξυπνη ενέργεια, ο έξυπνow φωτισμόw, h έξυπνη κινητικότητα, h έξυπνη διαχείριση των υδάτων κ.λπ. Η βασική υποδομή των παραπάνω βασίζεται σε διασύνδεση αισθητήρων, ενεργοποιητών, και ηλεκτρονικών συστημάτων, τα οποία φέρουν λογισμικό, δεδομένα, υποστηρίζουν την σύνδεση στο Internet και σε Η/Υ. Το IoT εφαρμόζεται για τη βελτίωση όλων αυτών των συστημάτων που δημιουργούν μια

έξυπνη πόλη, και είναι αυτόνομοι και διαλειτουργικοί, ασφαλείς και αξιόπιστοι. Η αλληλεπίδραση των συστημάτων εξαρτώνται από τον βαθμό της διασυνδεσιμότητας και της επικοινωνίας των συστημάτων.

Κεφάλαιο 2

IoT και Θέματα Ασφαλείας

2.1 Θεμελιώδεις έννοιες Ασφάλειας ΠΣ

Η Ασφάλεια Πληροφοριών (Information Security) ή η Ασφάλεια των Πληροφορικών Συστημάτων (Information System Security) είναι ο κλάδος της Πληροφορικής Επιστήμης που στοχεύει στην προστασία των πληροφοριακών πόρων ενός Πληροφοριακού Συστήματος (ΠΣ), από πιθανές ζημιές ή κακόβουλες ενέργειες, οι οποίες δύναται να προκαλέσουν άμεσα ή έμμεσα την μείωση της αξίας τους. Επίσης, η Ασφάλεια των ΠΣ αποσκοπεί στην παροχή αξιόπιστων πληροφοριών, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες όταν τις χρειάζονται [15]. Η διαφύλαξη των πληροφοριακών πόρων και δεδομένων βασίζεται στις αρχές των τριών θεμελιωδών ιδιοτήτων της Ασφάλειας Πληροφοριών. Οι ιδιότητες αυτές είναι γνωστές διεθνώς ως «CIA», και έχουν ως ακολούθως [16]:

- **Εμπιστευτικότητα (Confidentiality):** αφορά την προστασία της πληροφορίας από μη εξουσιοδοτημένη αποκάλυψή (ανάγνωση) της.

- **Ακεραιότητα (Integrity):** αφορά την προστασία της πληροφορίας από μη εξουσιοδοτημένη μεταβολή (τροποποίηση ή διαγραφή) της.

- **Διαθεσιμότητα (Availability):** αφορά τη διαφύλαξη της εξουσιοδοτημένης πρόσβασης (είτε για αποκάλυψη είτε για μεταβολή) στην πληροφορία, χωρίς εμπόδια ή καθυστέρηση.

Βασικοί Ορισμοί στην Ασφάλεια ΠΣ

Αγαθό (asset) είναι κάθε αντικείμενο (υπολογιστικός ή δικτυακός πόρος ή δεδομένα), το οποίο έχει **Αξία** (value) για τον **Ιδιοκτήτη** (owner) του και για αυτό το λόγο πρέπει να προστατευτεί από την περιστασιακή ή μόνιμη απώλειά του. Ένα αγαθό μπορεί να εκτίθεται σε ένα **Κίνδυνο** (danger). Ο κίνδυνος αντιπροσωπεύει την αιτία για να περιοριστεί η αξία του αγαθού. Ο περιορισμός της αξίας του αγαθού ονομάζεται **Ζημιά** (harm). Κάθε κατάσταση που μπορεί να προκαλέσει ζημία σε ένα υπολογιστικό σύστημα, αποτελεί μια **Απειλή** (threat) γι' αυτό. Οι απειλές μπορούν να κατηγοριοποιηθούν σε **Φυσικές** απειλές (περιβαλλοντικές απειλές, π.χ. πυρκαϊά, πλημμύρα, σεισμοί, κλπ.), σε **Εκούσιες** απειλές που προκύπτουν εσκεμμένα από κακόβουλους χρήστες, και σε **Ακούσιες** απειλές που προκύπτουν ακούσιες και λανθασμένους χειρισμούς των χρηστών των υπολογιστικών συστημάτων.

Οι ζημίες σε ένα ΠΣ προκαλούνται μετά από **Επιθέσεις** (attack). Κάθε επίθεση εκμεταλλεύεται μία ή περισσότερες ευπάθειες του ΠΣ. Μια **Ευπάθεια** (vulnerability) αναφέρεται σε μια αδυναμία στις ρυθμίσεις ή τη διαχείριση του συστήματος ή ένα ευάλωτο σημείο σε ένα υποσύστημα ασφάλειας.

Η κατηφοριοποίηση των ευπαθειών έχει συνοπτικά ως ακολούθως:

- **Ανθρώπινες Ευπάθειες:** αποτελούν την κρισιμότερη κατηγορία για την ασφάλεια ενός ΠΣ. Είναι οι χειρότερες καθώς δύναται να προκαλέσουν τις χειρότερες επιπτώσεις, αφού προέρχονται από χρήστες που γνωρίζουν καλά το ΠΣ.
- **Ευπάθειες Υλικού και Λογισμικού:** αφορούν προβληματική κατασκευή, καθώς και λανθασμένες ρυθμίσεις και δυσλειτουργίες του υλικού (hardware) και του λογισμικού (software).
- **Ευπάθειες Μέσων:** αφορούν προβληματικές διαδικασίες διαχείρισης που μπορεί να οδηγήσουν σε κλοπή ή καταστροφή μαγνητικών, οπτικών ή έντυπων μέσων αποθήκευσης δεδομένων.

- **Ευπάθειες Επικοινωνιών:** αφορούν κατασκευαστικές αδυναμίες, λανθασμένες ρυθμίσεις, καθώς και δυσλειτουργίες των δικτυακών συνδέσεων.
- **Φυσικές Ευπάθειες:** αφορούν το φυσικό χώρο όπου αναπτύσσονται και λειτουργούν τα συστήματα (π.χ. datacenters).
- **Φυσικές Ευπάθειες:** αφορούν φυσικά φαινόμενα (π.χ. φυσικές καταστροφές), περιβαλλοντικές εξαρτήσεις κ.ά.

2.1.1 Επιθέσεις κακόβουλου λογισμικού

Κάθε φορά που ένας κακόβουλος χρήστης (cracker ή hacker όπως συνηθίζεται να λέγεται) στοχεύει να εισβάλλει σε ένα ΠΣ, πάντοτε συλλέγει πληροφορίες γύρω από αυτό, ώστε ψηφιακά να εισβάλλει ευκολότερα στο σύστημα αποκρύπτοντας και την ταυτότητάς του. Η συλλογή των πληροφοριών έχει να κάνει συνήθως με κωδικούς πρόσβασης, διευθύνσεις, πληροφορίες για τους διαχειριστές του συστήματος, το hardware, το software, το firmware υπολογιστικών πόρων κλπ. Για την προσβολή του ΠΣ ο κακόβουλος χρήστης πραγματοποιεί επιθέσεις, που στοχεύουν στην εκμετάλλευση ευπαθειών του ΠΣ.

Τα κυριότερα κακόβουλα εργαλεία - λογισμικά που χρησιμοποιεί ο κακόβουλος χρήστης για τις επιθέσεις του είναι:

Packet Sniffer ή **Packet Analyzer:** λογισμικό που χρησιμοποιείται για να υποκλέψει και να ερμηνεύσει πληροφορίες από τα πακέτα δεδομένων που εισέρχονται σε ένα δίκτυο υπολογιστών και εξέρχονται από αυτό. Τα packet sniffers καταγράφουν την κίνηση (*traffic*) των πακέτων, συλλαμβάνουν το καθένα από αυτά και τέλος, αν χρειάζεται, αποκρυπτογραφούν τα δεδομένα τους δίνοντας ποικίλες πληροφορίες στον hacker. Αξίζει να σημειωθεί ότι κάθε φορά που στέλνουμε πληροφορίες ή δεδομένα μέσω του (δια)δικτύου, αυτά κωδικοποιούνται και μεταφέρονται ως πακέτα για λόγους ασφαλείας.

- **Δούρειος Ίππος (Trojan Horse):** Ο όρος προέρχεται από την ομώνυμη κατασκευή που χρησιμοποιήθηκε στην ελληνικη μυθολογία. Αναφέρεται σε κακόβουλο λογισμικό που έχει τη δυνατότητα να κρύβεται μέσα σε κάποιο καλόβουλο λογισμικό, ώστε να γίνεται δύσκολα αντιληπτό από το ΠΣ. Έτσι, ο ανυποψίαστος χρήστης του συστήματος το χρησιμοποιεί ως ένα κοινό (*ασφαλές*) πρόγραμμα και ουσιαστικά του παρέχει πληροφορίες για αυτόν, όπως για παράδειγμα usernames, passwords, logs, e-mais, κλπ. Τέλος, οι πληροφορίες αυτές μεταβιβάζονται στον κακόβουλο χρήστη.

- **Απομακρυσμένη Διαχείρηση (Backdoor και Remote Administration**): είναι κακόβουλα λογισμικά τα οποία εγκαθιστώνται σε ένα υπολογιστικό σύστημα κρυφά, συνήθως μέσω των trojan horses. Αυτά δίνουν σε τρίτους τη δυνατότητα να εισβάλλουν σε αυτά τα συστήματα μέσω του διαδικτύου και να μπορούν σχεδόν πλήρως να τα διαχειρίζονται. Χρησιμοποιούνται συχνά για παρακολουθήσεις και για καταγραφή πληροφοριών. Σκοπός τους είναι, επίσης, να παραμένουν μη-ανιχνεύσιμα.

- **Σκουλήκια (Worms) και Ιοί (Viruses)**: είναι κακόβουλα προγράμματα διαφορετικά μεταξύ τους και διαφορετικά απο τους Δούρειους Ίππους. Τα σκουλήκια έχουν τη δυνατότητα να εξαπλώνονται από υπολογιστή σε υπολογιστή χωρίς να απαιτείται ανθρώπινη ενέργεια, λαμβάνοντας πληροφορίες για το τρόπο μεταφοράς των αρχείων μεταξύ αυτών. Όταν ένα σκουλήκι ταξιδεύει σε ένα δίκτυο και αντιγράφει τον εαυτό του συνεχώς, απαιτεί περισσότερη μνήμη από το σύστημα και συνήθως αυτό καταρρέει. Ένας ιός (*virus*) "κολλάει" σε ένα αρχείο ή πρόγραμμα, συνήθως εκτελέσιμο και έχει τη δυνατότητα να μεταφέρεται από σύστημα σε σύστημα, αφήνοντας "μολύνσεις" πίσω του. Σε αντίθεση με τα σκουλήκια (*worms*), ο ιός απαιτεί ανθρώπινη ενέργεια, για παράδειγμα, μπορεί να υπάρχει σε ένα υπολογιστικό σύστημα χωρίς όμως να το μολύνει, μέχρι ο χρήστης να εκτελέσει το αρχείο που τον περιέχει. Έτσι οι χρήστες, ανυποψίαστοι, εξαπλώνουν τον ιό ο οποίος μπορεί να δημιουργήσει καταστροφές σε αρχεία, στο software αλλά και στο hardware.

- **Denial of Service (DoS) και Distributed Denial of Service (DDoS)**: πρόκειταιγια μεθόδους επιθέσεων που υπολοποιούνται από διάφορα προγράμματα και στοχεύουν να κάνουν μια διαδικτυακή υπηρεσία ή έναν εξυπηρετητή να καταρρεύσει, δηλαδή να αδυναμεί να εξυπηρετήσει τις απαιτήσεις ενός χρήστη. Σε μία **DoS** επίθεση, ο υπολογιστής του κακόβουλου χρήστη (*attacker*) αποστέλλει ένα μεγάλο πλήθος δεδομένων (*πακέτων*) στο επιτιθέμενο δίκτυο (*server* ή *website*) με αποτέλεσμα να το υπερφορτώσει ή να το αναγκάσει να επανεκκινήσει την λειτουργία του (*πιθανή απώλεια δεδομένων*). Προσπαθεί, δηλαδή, να το "γεμίσει" (*flood*) με απαιτήσεις (*requests*) τις οποίες το σύστημα αδυναμεί να διαχειριστεί/εκτελέσει. Συνεπώς, κάποιος άλλος χρήστης δεν έχει πλέον την δυνατότητα να το προσπελάσει. Σε μία **DDoS** επίθεση, ο hacker, προσπαθεί να εισβάλλει σε πολλούς υπολογιστές και να πάρει τον έλεγχο τους στα χέρια του. Αφού το καταφέρει, αναγκάζει τον καθένα από αυτούς να εκτελέσει μια επίθεση DoS στο επιθυμητό δίκτυο. Δημιουργείται λοιπόν μια ισχυρή επίθεση χρησιμοποιώντας περισσότερους, από έναν, υπολογιστές (*πιο αποτελεσματική*). Και οι δύο τρόποι επιθέσεων συνήθως δεν οδηγούν στην υποκλοπή ή καταστροφή δεδομένων, όμως το διάστημα που ο server ή το δίκτυο δεν είναι διαθέσιμα, μπορούν να οδηγήσουν ενδεχομένως σε χρηματική ζημία των ιδιοκτητών.

- **Κοινωνική Μηχανική (Social Engineering)**: αποτελεί μέθοδο με την οποία ένας hacker μπορεί με "φυσικό" τρόπο να αποσπάσει χρήσιμες πληροφορίες απο ένα θύμα με διάφορα τεχνάσματα. Προσπαθεί δηλαδή να το ξεγελάσει παρουσιάζοντας τον εαυτό του ως κάποιο άλλο πρόσωπο στο οποίο ο επιτιθέμενος θα εμπιστευόταν αυτές τις πληροφορίες. Επιπρόσθετα, προβάλλοντας ποικίλα στοιχεία για αυτόν (ημερομηνία γέννησης, διεύθυνση, τηλέφωνο, αριθμούς λογαριασμών, κλπ.), τείνει να τον παραπλανήσει και να τον πείσει να δώσει στον hacker τα επιθυμητά στοιχεία. Χρησιμοποιεί ψέματα και "προκατασκευασμένα σενάρια" (*pretexting*), τα οποία δημιουργεί με έρευνα στη ζωή του θύματος πριν του επιτεθεί. Με αυτά αυξάνει συνήθως τις

πιθανότητες να αποσπάσει εύκολα αυτά που θέλει χωρίς να γίνει αντιληπτός. Αυτός που εφαρμόζει την κοινωνική μηχανική σπάνια έρχεται πρόσωπο με πρόσωπο με το άτομο που εξαπατά. Αντιθέτως, χρησιμοποιεί το τηλέφωνο, τα e-mails και συχνά ψεύτικες ιστοσελίδες στις οποίες τον παροτρύνει να εισάγει τα στοιχεία του και ύστερα να τα υποκλέψει (*μέθοδος phising*). Τον όρο social engineering διέδωσε ο Kevin Mitnick, πρώην hacker και αργότερα σύμβουλος ασφαλείας πληροφοριακών συστημάτων. Ο ίδιος ανέφερε ότι είναι πολύ ευκολότερο να ξεγελάσεις κάποιον να δώσει έναν κωδικό πρόσβασης για ένα σύστημα από το να προσπαθήσεις να τον σπάσεις.

- **SQL Injection:** χρησιμοποιείται για την εισαγωγή κακόβουλου κώδικα σε μια βάση δεδομένων SQL μέσα από πιθανές "τρύπες" ασφάλειας μιας ιστοσελίδας. Με αυτό το τρόπο, οι εγγραφές δεδομένων (*usernames, passwords, κλπ.*) που υπάρχουν στη βάση γίνονται εμφανείς στο άτομο που επιτέθηκε.

- **Cross-Site Scripting (XSS)**: επίθεση με την οποία γίνεται επίσης εκμετάλλευση των πιθανών τρωτών σημείων σε κάποιον ιστότοπο με εισαγωγή κώδικα HTML ή JavaScript. Τα προβλήματα που δημιουργούνται από αυτού του είδους τις επιθέσεις μπορεί να είναι προσωρινά ή μόνιμα και να ευθύνονται είτε στον εξυπηρετητή (*server*) είτε στον πελάτη (*client*). Στις παραδοσιακές επιθέσεις οι ευπάθειες οφείλονται στον server κατά την απαίτηση (*request*) κάποιας λειτουργίας από κάποιο script πρόγραμμα, ενώ οι βασισμένες σε DOM επιθέσεις συμβαίνουν στα στάδια επεξεργασίας περιεχομένου που εκτελούνται στον πελάτη. Το όνομα αυτών των επιθέσεων προέρχεται από τον τρόπο που απεικονίζονται τα HTML ή XML αντικείμενα ο οποίος αποκαλείται **DOM** (Document Object Model). Υπάρχουν επιπλέον, λογισμικά επιθέσεων που εμπεριέχονται σε άλλα, όπως τα **keyloggers** που καταγράφουν οτιδήποτε πληκτρολογείται σε έναν υπολογιστή και συμπεριλαμβάνονται συχνά στα trojan horses.

- **Brute-force attacks**: επιθέσεις όπου οι κακόβουλοι χρήστες δοκιμάζουν δηλαδή πολλούς συνδυασμούς κωδικών μέχρι να βρεθεί ο ζητούμενος. Τέλος, δεν αποκλείεται να υπάρχουν συσκευές (*hardware*) που μπορούν να εκτελέσουν κάποιες από αυτές τις επιθέσεις.

2.1.2 Η εποχή της Κυβερνο-Απειλής & Κυβερνο-ασφάλειας

Η λέξη **Κυβερνοχώρος** (Cyberspace) έγινε δημοφιλής στη δεκαετία του 1990, όταν οι χρήσεις του Διαδικτύου, της δικτύωσης και της ψηφιακής επικοινωνίας αυξανόταν δραματικά και ο όρος κυβερνοχώρος μπόρεσε να αντιπροσωπεύσει τις πολλές νέες ιδέες και φαινόμενα που εμφανίστηκαν. Δεν υπάρχει κάποιος σαφής ορισμός. Ονομάζουμε Κυβερνοχώρο σε γενικές γραμμές, τον μεγαλύτερο μη ρυθμιζόμενο και ανεξέλεγκτο τομέα, που προκύπτει από την διασύνδεση πληροφοριακών συστημάτων, στην ιστορία της ανθρωπότητας. Είναι επίσης μοναδικός διότι είναι ένας τομέας που δημιουργείται από τους ανθρώπους που αντιτίθενται στις παραδοσιακές φυσικές περιοχές [17].

Ενώ το IoT εισέρχεται ολοένα και περισσότερο στην καθημερινή ζωή, οι κίνδυνοι ασφαλείας που σχετίζονται με το Διαδίκτυο αυξάνονται και αλλάζουν ταχύτατα. Στον σημερινό κόσμο της τεχνολογίας που είναι συνεχώς εξελίσσεται και ενέχει ανεπαρκή επίγνωσης θεμάτων ασφαλείας από τους χρήστες, οι επιθέσεις στον κυβερνοχώρο δεν είναι πλέον θέμα «εάν» αλλά «πότε».

Οι κακόβουλοι χρήστες του κυβερνοχώρου εργάζονται σε νέες τεχνικές για να περάσουν την ΑΠΣ μεγάλων, καθιερωμένων οργανισμών και επιχειρήσεων,να προκαλέσουν ζημιά, να διαταράξουν ευαίσθητα δεδομένα ή να κλέψουν πνευματική ιδιοκτησία. Οι επιθέσεις τους γίνονται πιο εξελιγμένες και πιο δύσκολο να νικηθούν. Λόγω αυτής της συνεχιζόμενης ανάπτυξης, δεν μπορούμε να πούμε ακριβώς τι είδους απειλές θα προκύψουν το επόμενο έτος, σε πέντε χρόνια, ή σε 10 χρόνια. Μπορούμε μόνο να πούμε ότι αυτές οι απειλές θα είναι ακόμη πιο επικίνδυνες από αυτές του σήμερα. Μπορούμε επίσης να είμαστε σίγουροι ότι καθώς οι παλιές πηγές αυτής της

απειλής θα εξασθενίσουν, θα εμφανιστούν νέες πηγές για να πάρουν τη θέση τους. Παρά την αβεβαιότητα αυτή - στην πραγματικότητα, εξαιτίας αυτού - πρέπει να είμαστε σαφείς σχετικά με τον τύπο των απαραίτητων ελέγχων της ΑΠΣ.

Η αποτελεσματική ασφάλεια του κυβερνοχώρου είναι όλο και πιο πολύπλοκη. Οι λύσεις σημείων, ιδίως το λογισμικό εντοπισμού ιών, τα συστήματα IDS, το IPS, η επιδιόρθωση και η κρυπτογράφηση, παραμένουν βασικός έλεγχος για την καταπολέμηση των γνωστών επιθέσεων του σήμερα. Ωστόσο, καθίστανται λιγότερο αποτελεσματικές με την πάροδο του χρόνου, καθώς οι hackers / crackers βρίσκουν νέους τρόπους για να παρακάμψουν τους ελέγχους.

Η ασφάλεια στον κυβερνοχώρο είναι ένα ζήτημα για όλη την Επιχείρηση – Οργανισμό, και όχι μόνο ένας τεχνολογικός κίνδυνος. Τα παραδοσιακά αποδεδειγμένα μοντέλα διαχείρισης κινδύνου έχουν την προέλευση και τη φιλοσοφία τους εστιασμένα σε έναν κόσμο, όπου η Επιχείρηση / Οργανισμός κατέχει και κατέχει τα περισσότερα, αν όχι όλα, στοιχεία ενεργητικού (data assets) που ρέουν μέσω των συστημάτων. Η αυξανόμενη χρήση του Διαδικτύου και η κινητή εργασία σημαίνει ότι τα σύνορα της Επιχείρησης / Οργανισμού εξαφανίζονται: και ως εκ τούτου, το τοπίο κινδύνου καθίσταται επίσης απεριόριστο. Με την σημερινή πλειονότητα των Επιχειρήσεων / Οργασνισμών να διαθέτουν «διαδικτυακό φράχτη» αλλά να είναι ζωτικής σημασίας η επικοινωνία με τρίτους - επιχειρηματικούς τους συνεργάτες, γι 'αυτό πρέπει να δημιουργούν «τρύπες» στον φράχτη αυτό. Ως αποτέλεσμα, ένα σύστημα ασφάλειας στον κυβερνοχώρο θα πρέπει επίσης να περιλαμβάνει το ευρύτερο δίκτυο του οργανισμού, συμπεριλαμβανομένων των πελατών, των προμηθευτών / πωλητών, των συνεργατών, των επιχειρηματικών εταίρων, των κρατικών διαδικτυακών παροχών, των αποφοίτων τους, κ.α., που ονομάζονται όλα μαζί «επιχειρηματικό οικοσύστημα»

Ένα εκτεταμένο επιχειρηματικό οικοσύστημα διέπεται και διαχειρίζεται διάφορους παράγοντες με μεμονωμένες πολιτικές και απαιτήσεις διασφάλισης. Οι παράγοντες αυτοί έχουν μερικές φορές πολύ διαφορετικά συμφέροντα και επιχειρηματικούς στόχους στο πλαίσιο της συνεργασίας. Ως εκ τούτου, είναι

απαραίτητο να προσαρμοστεί η κανονική επικέντρωση του κινδύνου στον Οργανισμό για να ληφθεί αυτό υπόψη. Για να μπορεί ένας Οργανισμός να διαχειρίζεται αποτελεσματικά τους κινδύνους στο οικοσύστημα του, πρέπει να ορίσει σαφώς τα όρια αυτού του οικοσυστήματος.

Η διασύνδεση των ανθρώπων, των συσκευών και των οργανισμών στον σημερινό ψηφιακό κόσμο ανοίγει ένα εντελώς νέο πεδίο ευπάθειας,που αποτελούν

τα σημεία πρόσβασης στα οποία μπορούν να εισέλθουν οι εγκληματίες του κυβερνοχώρου. Το γενικό «τοπίο» κινδύνου του οργανισμού είναι μόνο ένα μέρος ενός δυνητικά αντιφατικού και αδιαφανή σύμπαντος των πραγματικών και δυνητικών απειλών που προέρχονται πολύ συχνά από εντελώς απροσδόκητους και απρόβλεπτους παράγοντες απειλής, έχουν κλιμακωτή επίδραση.

Ακολουθούν μερικά παραδείγματα Κυβερνοαπειλής – Κυβερνοασφάλειας σε έννοιες και δομές της Επιστήμης των Υπολογιστών και της Πληροφορικής:

- **Δίκτυα Έξυπνων Συσκευών**

Η υιοθέτηση των φορητών υπολογιστών οδήγησε σε θολάρια οργανωτικά όρια, καθώς η πληροφορική φαντάζει να πλησιάζει περισσότερο τον χρήστη και να απομακρύνεται από τον οργανισμό. Η χρήση του Διαδικτύου μέσω των smartphones και των tablet (σε συνδυασμό με τις στρατηγικές "bring-your-own-device - BYOD" από τους εργοδότες) έχει καταστήσει τα δεδομένα ενός οργανισμού διαθέσιμα παντού και ανά πάσα στιγμή. Αναπόφευκτα, μια ευάλωτη συσκευή μπορεί να οδηγήσει σε άλλες ευάλωτες συσκευές και είναι σχεδόν αδύνατο να καλύψει όλες τις ευπάθειες για όλες τις συσκευές. Για τους εγκληματίες του κυβερνοχώρου, δεν θα είναι δύσκολο να βρεθεί ένας στόχος για την επίθεσή τους. Η αγορά της ευπάθειας (η υπόγεια μαύρη αγορά που πωλεί botnets, rootkits, κλπ.) είναι τεράστια. Για παράδειγμα, είναι ευκολότερο για έναν εισβολέα να εγκαταστήσει ένα "Trojan" σε ένα τηλέφωνο, αν το τηλέφωνο συνδέεται με τον υπολογιστή που έχει ήδη παραβιαστεί. Με ακόμη περισσότερες

συσκευές συνδεδεμένες, θα είναι ακόμα ευκολότερο για έναν κακόβουλο χρήστη να επιτεθεί.

- **Υποδομές ΠΣ (Infrastructure)**

Στα παραδοσιακά κλειστά συστήματα λειτουργικής τεχνολογίας παρέχονται ολοένα και περισσότερες διευθύνσεις IP, οι οποίες είναι προσβάσιμες εξωτερικά, έτσι ώστε οι απειλές στον κυβερνοχώρο να απομακρύνονται από τα back office συστήματα και σε κρίσιμες υποδομές, όπως συστήματα παραγωγής και μεταφοράς ενέργειας και άλλα συστήματα αυτοματισμού.

- **Υπολογιστικό Νέφος (Cloud Computing)**

Το Cloud computing αποτελεί απαραίτητη προϋπόθεση και συστατικό, θα λέγαμε, για το Διαδίκτυο από τις πρώτες ημέρες της εξέλιξής του. Το σύννεφο παρέχει μια πλατφόρμα για να ακμάσει το Διαδίκτυο, ωστόσο, υπάρχουν ακόμα πολλές προκλήσεις τις οποίες αντιμετωπίζουμε σήμερα, όταν πρόκειται για την ασφάλεια του cloud ή την ασφάλεια των δεδομένων στο σύννεφο. Οι οργανισμοί συχνά ανακαλύπτουν πολύ αργά ότι τα πρότυπα ασφαλείας του παρόχου σύννεφων τους μπορεί να μην αντιστοιχούν στις δικές τους. Τα πρόσφατα συμβάντα του "CelebGate" και ο συμβιβασμός του IAAS του Amazon είναι τα ζωντανά παραδείγματα τέτοιων ατελειών. Αυτά είναι τα περιστατικά που οδήγησαν τους επικριτές να ονομάσουν αυτές τις υπηρεσίες ως ενιαίο σημείο hack, αντί για ένα μόνο σημείο αποθήκευσης.

Με το Big Data να είναι ήδη προ των πυλών της σύγχρονης εποχής, θα υπάρξει ένα τεράστιο ποσό των δεδομένων που παράγονται για τους παρόχους υπηρεσιών επίσης. Με την πληθώρα των δεδομένων που θα έχουν, οι διακομιστές αποθήκευσης θα πρέπει να ενημερώνονται και να ασφαλίζονται συνεχώς. Αυτό αποφέρει αύξηση των κινδύνων για επικοινωνιακές συνδέσεις, δεδομένου ότι οι αισθητήρες και οι συσκευές θα επικοινωνούν και θα λειτουργούν με ευαίσθητα προσωπικά στοιχεία όλη την ώρα στα κανάλια. Με τα δεδομένα που αποθηκεύονται σε αυτές τις υπηρεσίες cloud, υπάρχει επίσης ο κίνδυνος να αυξηθεί το spam, καθώς οι διακομιστές

σύννεφων μετακινούνται ουσιαστικά από μια γεωγραφική τοποθεσία στην άλλη σε λίγα λεπτά, ανάλογα με την απαίτηση.

2.2 Ιδιωτικότητα στο IoT

Η δυνατότητα ενός ατόμου ή μιας ομάδας ατόμων να απομονώνουν – αποκρύψουν πληροφορίες σχετικές με το άτομο ή την ομάδα, είναι αυτό που καλείται **Ιδιωτικότητα**. Μερικές φορές η ιδιωτικότητα σχετίζεται με την ανωνυμία, δηλαδή την επιθυμία να παραμείνει κάποιος απαρατήρητος ή μη αναγνωρισθείς στο κοινό. Ο βαθμός με τον οποίο ιδιωτικές πληροφορίες εκτίθενται εξαρτάται από το πως το κοινό θα εκλάβει αυτές τις πληροφορίες. Η ιδιωτικότητα είναι ευρύτερη από την ασφάλεια και περιλαμβάνει τις έννοιες της κατάλληλης χρήσης και προστασίας των πληροφοριών [18].

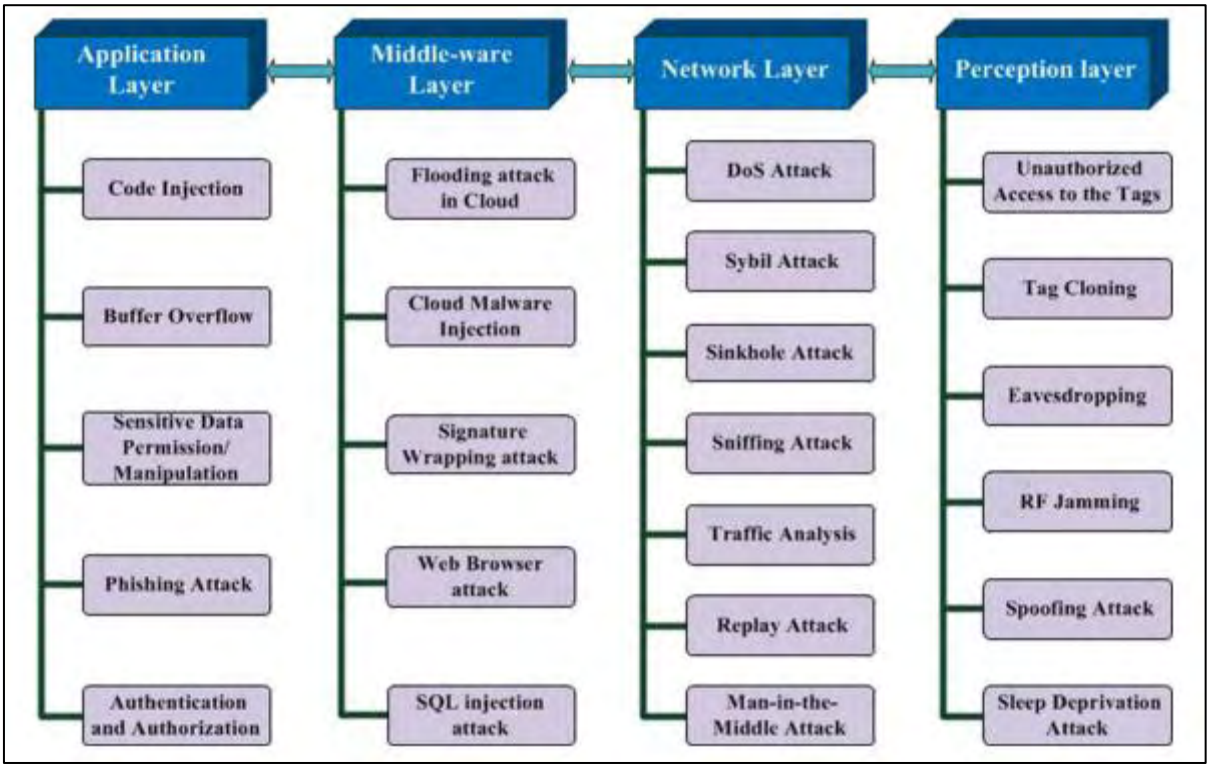
Στην Πληροφορική, ιδιωτικότητα της πληροφορίας (information privacy) ή Ιδιωτικότητα των δεδομένων (data privacy) δεν είναι πολύ καλά αποσαφηνιμένος όρος, όπως συμβαίνει και γενικά με τον προσδιορισμό της έννοιας ιδιωτικότητα. Ουσιαστικά η ιδιωτικότητα της πληροφορίας αναφέρεται στην συσχέτιση μεταξύ της συλλογής και της διάδοση των δεδομένων, με την τεχνολογία και τις υπολογιστικ΄ς μηχανές, αλλά και με το νομικό πλαίσιο του τι περιλαμβάνει η ιδιωτικότητα ενός ατόμου ή μιας ομάδας. Είναι χαρακτηρισστικό της Πληροφορίκής και της Τεχνολογία ότι παρέχονται πλατφόρμες και εφαρμογές για κοινή χρήση δεδομένων, μέσα στις οποίες όμως προστατεύονται ταυτόχρονα και οι προσωπικές πληροφορίες του ατόμου. Ως προσωπικές πληροφορίες, ορίζονται αυτές που μπορούν να χρησιμοποιηθούν, ώστε να ταυτοποιηθεί το άτομο. Στο σημείο αυτό, εισέρχεται το γνωστικό αντικείμενο της Ασφάλειας των Πληροφοριακών Συστημάτων για να χρησιμοποιήσει υπολογιστικό υλικό, λογισμικό και ανθρώπινους πόρους για να αντιμετωπίσουν αυτό το ζήτημα της ιδιωτικότητας της πληροφορίας. Βεβαίως, η δυνατότητα να ελέγχει κάποιος στο IoT (και ουσιαστικά στο Internet) ποιες

πληροφορίες αποκαλύπτονται για τον ίδιον, και ποιος μπορεί να έχει πρόσβαση σε αυτές τις πληροφορίες, αποτελεί ένα ζήτημα αυξανόμενης ανησυχίας.

Στο σημείο αυτό, πρέπει να σημειωθεί ότι η ιδιωτικότητα της πληροφορίας αποτελεί σημαντικό θέμα στις Επιχειρήσεις και μεγάλους Οργαμισμούς (κρατικούς, νοσκομεία, κ.α.). Η ιδιωτικότητα της πληροφορίας στις επιχειρήσεις / οργανισμούς επικεντρώνεται στην διασφάλιση των προσωπικών δεδομένων από μη εξουσιοδοτημένο χρήστη, καθώς και στην διαφύλαξη της εμπιστοσύνης των πελατών με την παρεμπόδιση της κακόβουλης δραστηριότητας, π.χ. της κλοπής προσωπικών δεδομένων, ευαίσθητων προσωπικών δεδομένων (δεδομένα υγείας), την αποστολή ανεπιθύμητης αλληλογραφίας (spamming) και το ηλεκτρονικό «ψάρεμα» (phishing). Οι πληροφίες των πελατών της επιχείρησης μπορεί να είναι είτε δεδομένα χρήστη, που αποτελούν πληροφορίες που συλλέγονται από την επιχείρηση (δεδομένα που συμπληρώνεται σε εφαρμογές από τον ίδιο τον χρήστη, δεδομένα που συλλέγονται έμμεσα και είναι τα μεταδεδομένα, δεδομένα συμπεριφοράς χρήσης, κ.α.), είτε προσωπικά δεδομένα.

2.3 Ταξινόμηση επιθέσεων στο IoT

Βασικό ρόλο στην ταξινόμηση των επιθέσεων που μπορεί ένας κακόβουλος χρήστης να πραγματοποιήσει στο IoT, αποτελεί η αρχιτεκτονική του. Η ταξινόμηση των επιθέσεων ακολουθεί την αρχιτεκτονική του IoT και τα επίπεδα που αυτό διακρίνεται. Έτσι, η πρώτη εικόνα σχηματικά της ταξινόμησης φαίνεται ως παρακάτω (Εικόνα 9):



Εικόνα 9. Ταξινόμηση κακόβουλων επιθέσεων βασισμένο στα επίπεδα του IoT.

Επιθέσεις στο Application Layer

Οι επιθέσεις στο επίπεδο εφαρμογής στοχεύουν κυρίως στην μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα του χρήστη IoT. Οι επιτιθέμενοι προσπαθούν να εκμεταλλευτούν τις ευπάθειες των προγραμμάτων και των διαφόρων γενικά εφαρμογών (π.χ. με ένεση κώδικα, υπερχείλιση buffer, κ.α.). Μια προσέγγιση για να λάβει ένας μη εξουσιοδοτημένος πράκτορας την άδεια εισόδου σε μια εφαρμογή είναι η παραπλάνηση – παραχάραξη της ταυτότητας ενός έγκυρου χρήστη. Εκτός από αυτές τις επιθέσεις, το Application Layer απειλείται από ιούς, σκουλήκια και Trojans, άλλα και άλλα κακόβουλα προγράμματα, όπως Rootkit, spyware, adware, τα οποία επίσης υπονομεύουν την ιδιωτικότητα των χρηστών.

1. **Code Injection:** Αυτή η επίθεση συνεπάγεται την εισαγωγή κακόβουλου κώδικα χρησιμοποιώντας σφάλματα του προγράμματος μιας εφαρμογής, με σκοπό την

κλοπή δεδομένων, την απόκτηση ελεγχου του συστήματος και την μετάδοση worms. Οι πιο κοινές επιθέσεις περιλαμβάνουν ένεση κελύφους (shell injection) και ένεση με script HTML, επιφέροντας την παραπλάνηση της έγκυρης ιδιωτικότητας ή ακόμη και την πλήρη κατάρευση της εφαρμογής.

2. **Buffer Overflow:** Αυτή η επίθεση συνεπάγεται παραβίαση των ορίων του κώδικα ή δεδομένων μέσω της αξιοποίησης των τρωτών σημείων του προγράμματος. Πολλά προγράμματα λειτουργούν με μια προκαθορισμένη διάταξη μνήμης για τον κώδικα και τα δεδομένα του. Ο κακόβουλος χρήστης γράφει μια μακρά ακολουθία δεδομένων σε μια συγκεκριμένη περιοχή, με αποτέλεσμα την υπερχείλιση της ακολουθίας πέρα από την προκαθορισμένη περιοχή μνήμης. Το αποτέλεσμα μπορεί να είναι τροποποίηση άλλων δεδομένων, η εκτέλεση κακόβουλου κώδικα ή η καταστροφή της ροής ελέγχου του προγράμματος. Οι κοινές επιθέσεις στον κώδικα εφαρμογών περιλαμβάνουν stack / heap buffer overflow, format string attacks, σφάλμα σε υπολογισμό integer ή double. Το buffer overflow είναι η συχνότερη επίθεση σε λογισμικό, και μπορεί να επιτρέψει σε έναν μη εξουσιοδοτημένο χρήστη να αποκτήσει δικαιώματα διαχειριστή και να εκτελέσει αυθαίρετο δικό του κώδικα.
3. **Sensitive Data Permission/Manipulation:** Αυτός ο τύπος κακόβουλης επίθεσης αναφέρεται σε παράνομη πρόσβαση και χειραγώγηση των ευαίσθητων δεδομένων, παραβιάζοντας την ιδιωτική ζωή του χρήστη ενός λογισμικού. Αυτή η επίθεση συνήθως εκμεταλλεύεται τις ελλείψεις σχεδιασμού στα δικαιώματα πρόσβασης των χρηστών στο λογισμικό [19]. Έχουν επιδειχθεί επιθέσεις που εκμεταλλεύονται το μοντέλο δικαιωμάτων στην διαχείριση των εφαρμογών σε SmartHomes [20]. Επιπλέον, προηγούμενη έρευνα ανέλυσε τα γεγονότα που χρησιμοποιήθηκαν για την επικοινωνία μεταξύ SmartApp και SmartDevice. Σημειώνεται ότι τα SmartApps και το τα SmartDevices αποτελούν ένα ιδιαίτερα σημαντικό πρόβλημα στην ασφάλεια των δεδομένων και της ιδιωτικότητας. Ένα SmartDevice στέλνει ευαίσθητα δεδομένα στο SmartApp χρησιμοποιώντας συμβάντα (events). Το SmartApp χρησιμοποιεί events για παρακολούθηση του SmartDevice. Ωστόσο, λόγω της έλλειψης επαρκούς

προστασίας του event, αυτό μπορεί να προκαλέσει διαρροή της πληροφορίας του event, και να προκαλέσει σοβαρότερη ακόμη βλάβη στον χρήστη. Προκειμένου να επιλυθεί το πάνω από τα προβλήματα, έχει ήδη προταθεί ένα πλαίσιο προστασίας των ευαίσθητων δεδομένων, δηλώνοντας τα πρότυπα ροής των δεδομένων [21].

4. **Phishing Attack:** Στις επιθέσεις αυτές, ο κακόβουλος χρήστης προσποιείται ότι είναι πραγματικός - νόμιμος χρήστης σε μια εφαρμογή, με στόχο την λήψη ευαίσθητων πληροφοριών σχετικά με τους χρήστες της εφαρμογής, όπως κωδικούς πρόσβασης και στοιχεία πιστωτικών καρτών. Ο συνηθέστερος τρόπος εκτέλεσης της επίθεσης είναι το ηλεκτρονικό ταχυδρομείο (e-mail), όπου οι χρήστες ανοίγουν το μήνυμα και παρέχουν σε αυτό τις ευαίσθητες πληροφορίες που θέλει ο επιτιθέμενος [22],[23].
5. **Authentication and Authorization:** Ο μηχανισμός ελέγχου ταυτοποίησης – αυθεντικοποίησης ενός χρήστη σε μια εφαρμογή διαδραματίζει σημαντικό ρόλο για την προστασία των προσωπικών του πληροφοριών. Οι υπάρχοντες μηχανισμοί αυθεντικοποίησης δεν μπορούν να εγγυηθούν πλήρη πιστοποίηση στην ασφάλεια πληροφοριών χρήστη [24]. Ως αποτέλεσμα, οι εφαρμογές μπορούν να κατεβάσουν (download) κακόβουλα προγράμματα (payloads) όταν ενημερώνονται σε έκδοση, παρέχοντας απομακρυσμένη πρόσβαση στον κακόβουλο χρήστη σε μια συσκευή. Σε ένα άλλο παράδειγμα, η έλλειψη ενός τέλειου μηχανισμού ελέγχου ταυτότητας και αυθνετικότητας του χρήστη στην δομή ενός Smart Home, ο κακόβουλος χρήστης μπορεί να εκτελέσει μη εξουσιοδοτημένες πράξεις, όπως ανοίγοντας πόρτα (backdoor) στα λογισμικά του συστήματος [20].

Επιθέσεις στο Middleware Layer

Το ενδιάμεσο επίπεδο (Middleware Layer) παρέχει διασυνδέσεις και υπηρεσίες για το επίπεδο εφαρμογής. Ο κακόβουλος χρήστης μπορεί να επιτεθεί σε μια διαδικτυακή υπηρεσία (Web Service) για να επηρεάσει το επίπεδο εφαρμογής. Η επίθεση σε διακομιστή και στη βάση δεδομένων θα επηρεάσει την ασφάλεια των

πληροφοριών και την ασφάλεια λειτουργίας του συστήματος. Επιθέσεις στο cloud στοχεύουν κυρίως στην χρήση τεχνικών virtualization και στα δεδομένα. Ο στόχος της επίθεσης στο Middleware Layer είναι η καταστροφή της ποιότητας της υπηρεσίας (Quality of Service, QoS) και της ιδιωτικότητας των χρηστών.

1. **Flooding Attack in Cloud:** Αυτή είναι μια μορφή επιθέσεων άρνησης εξυπηρέτησης στο cloud (Cloud Denial of Service, CDoS). Οι κακόβουλοι χρήσες στέλνουν συνεχώς αιτήματα σε μια υπηρεσία στο το cloud, εξαντλώντας τους πόρους του και επηρεάζοντας την ποιότητα της υπηρεσίας (QoS). Όταν το cloud system διαπιστώσει ότι η τρέχουσα υπηρεσία δεν μπορεί να ανταποκριθεί στις απαιτήσεις, μεταφέρει την επηρεαζόμενη υπηρεσία σε άλλους διακομιστές (Cloud Servers). Αυτό οδηγεί σε αυξημένη πίεση εργασίας στους άλλους διακομιστές, με αυξημένη πιθανότητα κατάρρευσης του συστήματος και παροχής των υπηρεσιών cloud [25].
2. **Cloud Malware Injection:** Ο κακόβουλος χρήστης με αυτόν τον τρόπο επίθεσης μπορεί να τροποποιήσει δεδομένα, να αποκτήσει τον έλεγχο ενός συστήματος στο νέφος, και να εκτελέσει κακόβουλο κώδικα εισάγωντας μια κακόβουλη υπηρεσία ή μια κακόβουλη εικονική μηχανή (virtual Machine, VM) στο cloud ή να εκμεταλλευτούν ένα instance μιας cloud υπηρεσίας προς έναν χρήστη. Αποτέλεσμα είναι να μπορεί ο επιτιθέμενος να αποσπάσει ευαίσθητα δεδομένα μιας cloud υπηρεσίας [25].
3. **Signature Wrapping Attack:** Το cloud χρησιμοποιεί υπογραφή XML για να διασφαλίσει την ακεραιότητα της υπηρεσίας. Ο εισβολέας τροποποιεί υποκλεμμένα μηνύματα χωρίς να ακυρώνει την υπογραφή. Οι επιτιθέμενοι εκμεταλλεύονται τις ευπάθειες του πρωτοκόλλου SOAP για να τροποποιήσουν τα μεταφερόμενα ηλεκτρονικά μηνύματα. Επιπλέον, ένας εισβολέας με τον τρόπο αυτό της επίθεσης μπορεί να εκτελέσει αυθαίρετες εντολές και λειτουργίες ως νόμιμος χρήστης της υπηρεσίας cloud [26].
4. **Web Browser Attack:** Στο cloud, το πρόγραμμα περιήγησης Web χρησιμοποιείται για την εκτέλεση εντολών σε απομακρυσμένους διακομιστές,

όπως έλεγχος ταυτότητας και εξουσιοδότηση εντολές. Αλλά το ίδιο το πρόγραμμα περιήγησης δεν μπορεί να δημιουργήσει κρυπτογραφημένα σήματα XML. Οι hackers εκμεταλλεύονται αυτή την αδυναμία για να αποκτήσουν πρόσβαση χωρίς ταυτοποίηση - αυθεντικοποίηση. Η cloud υπηρεσία με βάση την υπηρεσία Web μπορεί να δημιουργήσει μερικά μεταδεδομένα (metadata), τα οποία περιέχουν ένα μεγάλο μέρος του περιεχομένου που σχετίζεται με την υπηρεσία cloud και την εφαρμογή της υπηρεσίας [26].

5. **SQL Injection Attack:** Με την ενσωμάτωση κώδικα SQL στα δεδομένα εισόδου, ένα ανεπαρκώς σχεδιασμένο πρόγραμμα μπορεί να είναι ευάλωτο σε τέτοιες επιθέσεις. Οι επιτιθέμενοι χρησιμοποιούν αυτές τα ερωτήματα – δηλώσεις SQL (SQL queries or statements) για την εμφάνιση, την τροποποίηση ή την διαγραφή των εμφανιζόμενων δεδομένων σε μια εφαρμογή. Αυτό το είδος της επίθεσης απειλεί ολόκληρες τις βάσεις δεδομένων και τα προσωπικά δεδομένα του χρήστη. Όταν διαδικτυακές εφαρμογές δέχονται επιθέσεις τύπου SQL Injection, η τρέχουσα σελίδα παρουσιάζει διαφορετικά αποτελέσματα σε σύγκριση με τις πραγματικές πληροφορίες [27],[28].

Επιθέσεις στο Network Layer

Υπάρχουν πολλά είδη δικτύων σε IoT, μεταξύ των οποίων το Διαδίκτυο και το Ασύρματο Δίκτυο Αοσθητήρων (Wireless Sensor Network, WSN). Τα διαφορετικά δίκτυα χρησιμοποιούν διαφορετικά πρωτόκολλα και συσκευές. Έτσι, και οι επιθέσεις στο επίπεδο δικτύου είναι επίσης ποικίλες. Η πιο κοινή επίθεση είναι η επίθεση DoS, η οποία μπορεί να εξαντλήσει τους πόρους του δικτύου και να επηρεάσει τη διαθεσιμότητα των υπηρεσιών του δικτύου. Η δικτυακή κίνηση μπορεί να αναλυθεί και να αναλυθούν και έτσι να υποκλαπούν επικοινωνίες. Με τον τρόπο αυτό, ένας κακόβουλος χρ'ηστης μπορεί να εκτελέσει και επίθεση επανάληψης. Εκτός αυτού, υπάρχουν και συγκεκριμένες επιθέσεις σε κόμβους δικτύου. Διακυβεύοντας έναν κόμβο δικτύου, εισβολείς μπορούν να αποκτήσουν μεταδιδόμενες πληροφορίες και να αποκτήσουν τον έλεγχο του δικτύου, όπως η επίθεση επανάληψης και η επίθεση κατά του ανθρώπου-μέσου.

1. **DoS Attack:** Στο δίκτυο, μια επίθεση Denial-of-service (επίθεση DoS) επιτυγχάνεται με την αποστολή αλλεπάλληλων αιτημάτων σε μια υπηρεσία δημιουργώντας ως εκ τούτου αυξημένη κυκλοφορία στο δίκτυο. Αυτός ο τύπος επίθεσης μπορεί να εξαντλήσει όλους τους διαθέσιμους πόρους, καθιστώντας τους πόρους του δικτύου μη διαθέσιμους στους χρήστες. Επιπλέον, πολλές μη κρυπτογραφημένες πληροφορίες των χρηστών μπορούν επίσης να διαρρεύσουν [7]. Εκτός αυτού, μια κατανεμημένη επίθεση άρνησης εξυπηρέτησης (Distributed DoS, DDoS) μπορεί να συνδυάσει πολλούς υπολογιστές ως επίθεση σε μία ενιαία πλατφόρμα επίθεσης και να ξεκινήσει επιθέσεις DDoS σε έναν ή περισσότερους στόχους [29]. Οι επιθέσεις DDoS επιτυγχάνουν αποτελεσματικότητα χρησιμοποιώντας πολλαπλά συστήματα υπολογιστών. Τα εξελιγμένα μηχανήματα μπορούν να περιλαμβάνουν υπολογιστές και άλλους δικτυακούς πόρους, όπως συσκευές IoT. Από ένα υψηλό επίπεδο, μια επίθεση DDoS είναι σαν μια κυκλοφοριακή συμφόρηση που κλείνει με αυτοκινητόδρομο, εμποδίζοντας την τακτική κίνηση να φτάσει στον επιθυμητό προορισμό της [30].
2. **Sybil Attack:** Ο τρόπος επίθεσης αυτός ονομάστηκε έτσι κατόπιν προτάσεως της Microsoft® το 2002. Σε μια επίθεση Sybil, ο επιτιθέμενος ανατρέπει το σύστημα φήμης ενός ομότιμου δικτύου, δημιουργώντας ένα μεγάλο αριθμό ψευδώνυμων ταυτοτήτων και τις χρησιμοποιεί για να κερδίσουν δυσανάλογα μεγάλη επιρροή. Η ευπάθεια ενός συστήματος φήμης σε μια επίθεση Sybil εξαρτάται από το πόσο φτηνά μπορούν να δημιουργηθούν ταυτότητες, από το βαθμό στον οποίο το σύστημα φήμης δέχεται εισροές από οντότητες που δεν έχουν αλυσίδα εμπιστοσύνης που τους συνδέει με μια αξιόπιστη οντότητα, και αν το σύστημα φήμης αντιμετωπίζει όλα οντότητες. Από το 2012, στοιχεία έδειξαν ότι οι επιθέσεις Sybil μεγάλης κλίμακας θα μπορούσαν να πραγματοποιηθούν με πολύ φθηνό και αποδοτικό τρόπο σε υπάρχοντα ρεαλιστικά συστήματα όπως το BitTorrent Mainline DH [31],[32].

3. **Sinkhole Attack:** Στην επίθεση αυτή οι hackers χρησιμοποιούν έναν δικτυακό κόμβο προσελκύοντας ροή δεδομένων από τους πιο κοντινούς κόμβους. Έτσι, το σύστημα κατά κάποιο τρόπο ξεγελιέται και θεωρεί ότι το δεδομένα που έχουν ήδη φθάσει στον προορισμό τους. Σε ένα ασύρματο δίκτυο αισθητήρων (WSN), το ο εισβολέας μπορεί να χρησιμοποιήσει κακόβουλο κόμβο για να προσελκύσει την κυκλοφορία δικτύου, και στη συνέχεια τα δεδομένα του αισθητήρα μπορούν να λειτουργούν κατά την βούληση του hacker. Γενικά, μια τέτοια επίθεση μια σημαντική απειλή για τα WSNs και θα πρέπει να θεωρηθεί ότι οι κόμβοι των αισθητήρων είναι κυρίως απλωμένοι σε ανοικτές περιοχές και με αδύναμη υπολογιστική ισχύ και ισχύ μπαταρίας.
4. **Sniffing Attack:** Οι επιτιθέμενοι χρησιμοποιούν συσκευές και εφαρμογές sniffer για να λάβουν πληροφορίες του δικτύου IoT, και στη συνέχεια εξαγάγουν πολύτιμα δεδομένα για περαιτέρω επιθέσεις [33].
5. **Traffic Analysis**: Οι επιτιθέμενοι χρησιμοποιούν εργαλεία ανάλυσης του φορτίου επικοινωνίας, ήτοι τον αριθμό και το μέγεθος των μεταδιδόμενων πακέτων. Όσο μεγαλύτερος είναι ο αριθμός των πακέτων που μπορεί να αναλυθεί, τόσο πιο πολύτιμες πληροφορίες θα είναι διαθέσιμες. Αυτός ο τύπος επίθεσης μπορεί να εφαρμοστεί σε κρυπτογραφημένα πακέτα. Από την ανάλυση της επικοινωνίας ενός Ασύρματου Δικτύου Αισθητήρων (WSN), μπορούν να εξαχθούν τρία είδη πληροφοριών. Πρώτον, ο κακόβουλος χρήστης μπορεί να εντοπίσει τη δραστηριότητα του δικτύου. Δεύτερον, ο κακόβουλος χρήστης μπορεί να αποκτήσει την φυσική θέση των σημείων ασύρματης πρόσβασης (Access Points, APs). Τέλος, ο κακόβουλος χρήστης μπορεί να μάθει τις πληροφορίες σχετικά με τον τύπο πρωτοκόλλου που χρησιμοποιείται στο διαδικασία μετάδοσης των πληροφοριών στο δίκτυο [33].
6. **Replay Attack:** Στον τρόπο επίθεσης αυτόν, οι κακόβουλοι χρήστες υποκλέπτουν πληροφορίες μεταξύ των δύο μερών του δικτύου. Τα ληφθέντα μηνύματα μεταδίδονται επανειλημμένα μεταξύ των ζευγών επικοινωνίας, ως

εκ τούτου εξαντλούν τους δικτυακούς πόρους επικοινωνίας. Στην τεχνολογία RFID, η επίθεση αυτή συμβαίνει συχνά στις επικοινωνίες μεταξύ του αναγνώστη και της ετικέτας RFID. Αυτός ο τύπος επίθεσης όχι μόνο καταναλώνει υπολογιστικούς πόρους μεταξύ του αναγνώστη και της ετικέτας, αλλά καταναλώνει επίσης τους πόρους της βάσης δεδομένων στο back-end σύστημα [34].

7. **Man-in-the-Middle Attack:** Αυτός ο τύπος επίθεσης είναι μια επίθεση σε πραγματικό χρόνο, που συμβαίνει μεταξύ δύο κόμβων του δικτύου, όταν ένας κακόβουλος χρήστης εισάγεται ως ενδιάμεσος και πληρεξούσιος σε μια επικοινωνιακή σύνοδο μεταξύ δύο συστημάτων στο δίκτυο. Ο κακόβουλος χρήστης κερδίζει την εμπιστοσύνη των δύο κόμβων και λαμβάνει πληροφορίες και για δύο κόμβους – μέρη επικοινωνίας [35].

Επιθέσεις στο Reception Layer

Το Reception Layer χρησιμοποιεί μεγάλο αριθμό τεχνολογιών αισθητήρων και ταυτοποίησης. Οι αισθητήρες – κόμβοι ενός δικτύου συνήθως είναι χρησιμοποιούν «ad hoc» δίκτυα για να αλλάζουν δυναμικά την τοπολογία του δικτύου. Οι κόμβοι αισθητήρων χρησιμοποιούν συχνά ασύρματη επικοινωνία λόγω της διαφορετικότητας των περιβαλλόντων που αναπτύσσονται, το οποίο είναι εκμεταλλεύσιμο από τους κακόβουλους χρήστες που δύναται να παρακολουθήσουν την επικοινωνία μεταξύ κόμβων. Αυτό, σε πιθανό συνδυασμό με το γεγονός ότι, μπορεί ένας hacker να έχει άμεσα φυσική πρόσβαση, η εκάστοτε επίθεση μπορεί να είναι αρκετά σοβαρή, όπως συμβαίνει στην κλωνοποίηση καρτών – ετικετών και σε ενέργειες πλαστογράφησης. Η τεχνολογία RFID χρησιμοποιείται ευρέως, και οι hackers μπορούν να καταστρέψουν την επικοινωνία μεταξύ του αναγνώστη και της ετικέτας RFID, π.χ. μέσω μπλοκαρίσματος του σήματος RF.

1. **Unauthorized Access to the Tags / Tag Cloning:** Τα συστήματα RFID δεν διαθέτουν αποτελεσματικές τεχνικές ταυτοποίησης, με αποτέλεσμα μη εξουσιοδοτημένους χρήστες μπορούν εύκολα να έχουν πρόσβαση στις ετικέτες - κάρτες. Στα ελεύθερα πρόσβασης WSNs, ο εισβολέας αποκτά πρόσβαση με τεχνικές «reverse engineering», με στόχο την υποκλοπή δεδομένων σε κάρτες RFID τεχνολογίας, και έπειτα την πλαστογράφησή τους ή την χρησιμοποίηση προσωπικών δεδομένων [36].
2. **RF Jamming:** Η ίδια η φύση της τεχνολογίας ραδιοσυχνότητας (RF) καθιστά τα ασύρματα δίκτυα LAN (WLAN) ανοιχτά σε μια ποικιλία μοναδικών επιθέσεων. Οι περισσότερες από αυτές τις επιθέσεις εκμεταλλέυονται το Layer 1 (Physical - PHY) και Layer 2 (Media Access Control - MAC) της προδιαγραφής 802.11. Ο κακόβουλος χρήστης, ως jammer, επιχειρεί να μπλοκάρει το φυσικό στρώμα του WLAN δημιουργώντας συνεχές θόρυβο υψηλής ισχύος κοντά στους ασύρματους κόμβους – δέκτες του IoT δικτύου, με σκοπό να επιτύχει την παρεμπόδιση μετάδοσης και καταγραφής της πληροφορίας με την εξάντληση των πόρων του δικτύου και της ενέργειας των κόμβων [37].
3. **Eavesdropping:** Χρησιμοποιώντας αυτό το είδος επιθέσεων, οι hackers παρακολουθούν απομακρυσμένα την ασύρματη επικοινωνία της συσκευής IoT και του κόμβου του δικτύου. Αν η επικοινωνία γίνεται με ένα σύστημα RFID τεχνολογίας, ο hacker χρησιμοποιεί μια κεραία για την υποκλοπή και καταγραφή των δεδομένων που ανταλλάσσονται μεταξύ των ασυρμάτως επικοινωνούντων ετικετών – καρτών και των αναγνωστών τους [38],[39].
4. **Spoofing Attack:** Σε συνέχεια του προηγούμενου τρόπου επίθεσης, οι hackers με αρκετές γνώσεις στα πρωτόκολλα επικοινωνίας και αυθεντικοποίησης – ταυτοποίησης χρήστη, εφαρμόζουν τεχνικές για να προσποιηθούν έγκυρο χρήστη κάρτας και να αναγκάσουν την επανάληψη των διαδικασιών τατυτοποίησης σε ένα σύστημα επικοινωνίας κάρτας – αναγνώστη, με σκοπό την εξάντληση των πόρων του δικτύου και της ενέργειας του κόμβου [39].

5. **Barrage Attack / Sleep Deprivation Attack:** Το Perception Layer είναι σχετικά περιορισμένο σε πόρους και ενέργεια, γι΄αυτό και κάθε κόμβος δικτύου χρησιμοποιεί «sleep mode» για να παραταθεί η ενεργειακή ισχύς. Εκμεταλλευόμενοι αυτήν την αδυναμία, οι κακόβουλοι χρήστες στοχεύουν να διατηρήσουν τον κόμβο σε κατάσταση λειτουργίας για την γρήγορη εξάντληση της ενέργειας, που αποσκοπεί στην αποκοπή της επικοινωνίας των κόμβων που μεταδίδουν και συλλέγουν δεδομένα [40].

2.4 Στοιχεία Ασφάλειας στην IoT Νεφοϋπολογιστική

Σύμφωνα με με τον Zhou, Dong & Vassilako, ανάλογα με την λειτουργικότητα των συσκευών και των υπηρεσιών IoT, έχουμε το «στατικό», εννοώντας υπηρεσίες Cloud κυρίως αλλά και σταθερές συσκευές μετάδοσης πληροφορίας (π.χ. σταθερές IP κάμερες, sensors), και το κινητό IoT, όπου ουσιαστικά μετέχουν οι κινητές συσκευές και τεχνολογίες (π.χ. κινητά τηλέφωνα, mobile-Health technology, αυτοκίνητα connected με το Internet, αεροπλάνα, κλπ.). Συγκεκριμένα αναφέρουν ότι «According to the functionality, cloud-based IoT can be categorized into static and mobile, the latter of which is more challenging in protocol design». Η ταχεία ανάπτυξη της κινητής τηλεφωνίας, η επόμενη γενιά τεχνολογίας δικτύων όπως η πέμπτη γενιά (5G), καθώς και το Cloud-based IoT, έφερε στο προσκήνιο θέματα ασφάλειας και προστασίας δεδομένων. Πέρα από την γνωστή εμπιστευτικότητα που πρέπει να υπάρχει στα δεδομένα του IoT, οι απαιτήσεις σε ασφάλεια στην νεφοϋπολογιστική του IoT (Cloud-based IoT Threats) είναι γενικώς ως εξής [41]:

Identity Privacy: Αναφέρεται στο γεγονός ότι η ταυτότητα του χρήστη της κινητής συσκευής IoT είναι πραγματική και πρέπει να προστατεύεται σωστά. Αν και η τεχνική των ψευδώνυμων έχει υιοθετηθεί ευρέως για την επίτευξη αυτού του στόχου, δεν μπορεί να αντισταθεί στον δυναμικό εντοπισμό για το απόρρητο τοποθεσίας.

Location Privacy: Το απόρρητο της τοποθεσίας φαίνεται ιδιαίτερα κρίσιμη, δεδομένου ότι τα συχνά εκτεθειμένα η ιδιωτικότητα της τοποθεσίας θα αποκαλύψει τη συνήθεια

ζωής τον χρήστη του IoT. Η τεχνική της ψευδωνυμοποίησης για την απόκρυψη της θέσης ενός χρήστη είναι ευρέως διαδεδομένη, όπως αναφέρθηκε και παραπάνω, αλλά υπάρχουν αλγόριθμοι που μπορεί να χρησιμοποιήσει ένας κακόβουλος χρήστης για να γεω- εντοπίσει ένα άλλον χρήστη IoT.

Node Compromise Attack: Η επίθεση συμβιβασμού – κόμβου αναφέρεται στο ότι ο κακόβουλος χρήστης αποσπά όλες τις ιδιωτικές πληροφορίες από τις συσκευές IoT (από τους πόρους δηλαδή), αντικαθιστώντας τες με κακόβουλες συσκευές που είναι υπό τον έλεγχό του. Τέτοιες πληροφορίες μπορεί να περιλαμβάνουν τα κρυφά κλειδιά κρυπτογράφησης των πακέτων της πληροφορίας, το ιδιωτικό κλειδί παραγωγής ψηφιακών υπογραφών, κ.α.

Layer Removing/Adding Attack: Αυτή η επίθεση συμβαίνει όταν μια ομάδα χρηστών IoT αφαιρεί ή προσθέτει επίπεδα προώθησης μεταξύ τους, μειώνοντας ή μεγιστοποιώνοντας τον αριθμό των ενδιάμεσων πομπών.

Forward and Backward Security: Λόγω της κινητικότητας και της δυναμικής διαμόρφωσης μιας κοινωνικής ομάδας στο IoT, είναι απαραίτητο να επιτευχθεί ασφάλεια στην αποστολή και λήψη της πληροφορίας. Το πρώτο (forward security) σημαίνει ότι οι πρόσφατα συνδεδεμένοι χρήστες IoT μπορούν μόνο να αποκρυπτογραφήσουν το κρυπτογραφημένο μηνύματα που ελήφθησαν μετά, αλλά όχι πριν από την ένταξή τους στην ομάδα. Αντιθέτως, το δεύτερο (backward security) σημαίνει ότι οι ανακαλούμενοι στην ομάδα χρήστες IoT μπορούν μόνο να αποκρυπτογραφήσουν τα κρυπτογραφημένα μηνύματα πριν αλλά όχι μετά την αναχώρησή τους.

Semi-Trusted and/or Malicious Cloud Security: Το ημι-αξιόπιστο μοντέλο προστασίας στη νεφοϋπολογιστική του IoT σημαίνει ότι το σύννεφο συμμορφώνεται με τις προδιαγραφές ασφαλείας, αλλά προσπαθεί κρυφά να εξάγει τις ιδιωτικές πληροφορίες απο τις αλληλεπιδράσεις των χρηστών IoT. Ενώ, το κακόβουλο μοντέλο προστασίας σημαίνει ότι ο κακόβουλος χρήστης (π.χ. διαχειριστής του συννέφου)

μπορεί να καταστρέψει αυθαίρετα τα πρωτόκολλα επεικοινωνίας. Για τον λόγο αυτό, πρέπει να διασφαλίζονται τα κάτωθι:

- Input privacy: Τα δεδομένα εισαγωγής από καλοπροαίρετο χρήστη του cloud πρέπει να είναι καλά προστατευμένα από την συνέργια μεταξύ του συννcloudέφου και εξουσιοδοτημένων αποδεκτών της πληροφορίας.
- Output privacy: Οποιοδήποτε αποτέλεσμα εξαγώμενης πληροφορίας από το cloud, θα πρέπει να αποκρυπτογραφείται με επιτυχία εγκεκριμένους δέκτες δεδομένων σε αυτό.
- Function privacy: Η υποκείμενη λειτουργία πρέπει να προστατεύεται καλά από τον συνδυασμό της νεφοϋπολογιστικής και των κακόβουλων χρηστών IoT.

Η επέκταση της νεφοϋπολογιστικής (Cloud Computing) είναι και αυτή ραγδαία ως απόρροια του Διαδικτύου. Σε πολλές περιπτώσεις, η τεχνολογία Cloud παρέχει το ενδιάμεσο στρώμα μεταξύ των πραγμάτων του IoT και των εφαρμογών του IoT, κρύβοντας την πολυπλοκότητα και τις λειτουργίες που είναι απαραίτητες. Επίσης, μπορεί προσφέρει απομακρυσμένη αποθήκευση πληροφορίας και ανάπτυξη και εκμετάλλευση διαφόρων εφαρμογών δια μέσου του Διαδικτύου. Με βάση αυτά, ο συνδυασμός IoT και τεχνολογία Cloud προσφέρουν κίνητρα χρησιμοποίησης, αλλά εγείρουν ταυτόχρονα πολλά θέματα ασφαλείας. Όταν σημαντικές εφαρμογές στο IoT περιβάλλον χρησιμοποιούν τεχνολογία Cloud, αυτομάτως εγείρονται ερωτήματα σχετικά με τις υποχρεώσεις και τις συμφωνίες επιπέδου υπηρεσιών (Service Level Agreements – SLAs) μεταξύ των παρόχων και των ιδιοκτητών των εφαρμογών και των ιδιοκτητών της αποθήκευσης των δεδομένων σε φυσικούς εξυπηρετητές [42].

Τα κυριότερα θέματα ασφαλείας στην νεφοϋπολογιστική του IoT έχουν να κάνουν με τα εξής [43]:

1. **Ετερογένεια:** Μία μεγάλη πρόκληση στην ενσωμάτωση της τεχνολογίας Cloud στο IoT σχετίζεται με την ευρεία ετερογένεια των διαθέσιμων συσκευών,

λειτουργικών συστημάτων, πλατφορμών και υπηρεσιών που χρησιμοποιούνται για την ανάπτυξη και εκμετάλλευση εφαρμογών.

2. **Απόδοση:** Οι εφαρμογές Cloud και οι αρχιτεκτονικές IoT εισάγουν συγκεκριμένες επιδόσεις και απαιτήσεις Quality of Service σε διάφορα επίπεδα (π.χ. στην επικοινωνία, στην επεξεργασία – μετάδοση – αποθήκευση της πληροφορίας).
3. **Αξιοπιστία:** Ο συνδυασμός νεφοϋπολογιστικής και IoT για κρίσιμες εφαρμογές εγείρει θέματα αξιοπιστίας, που συνήθως προκύπτουν στο πλαίσιο της έξυπνης κινητικότητας. Για παράδειγμα, συσκευές και οχήματα που κινούνται συχνά, με αποτέλεσμα η δικτύωση και η επικοινωνία μεταξύ των συσκευών και οχημάτων να είναι συχνά διαλείπουσα, επιφέροντας αναξιοπιστία στην λειτουργικότητα.
4. **Μεγάλα δεδομένα (Big Data):** Με τον αυξανόμενο αριθμό διασυνδεδεμένων συσκευών στο Διαδίκτυο, είναι ανάγκη να δοθεί ιδιαίτερη προσοχή στη μεταφορά, αποθήκευση, πρόσβαση και επεξεργασία των τεραστίων σε ποσότητα πληροφορικής δεδομένων που παράγονται και διακινούνται. Η πανταχού παρούσα κινητή συσκευή και η διαπερατότητα των αισθητήρων, πράγματι απαιτούν κλιμακούμενες πλατφόρμες υπολογιστών.
5. **Παρακολούθηση:** Στην τεχνολογία Cloud πρέπει να υπάρχει συνεχής παρακολούθηση των υπολογιστικών πόρων στο σύννεφο, της διαθέσιμης χωρητικότητας, και των αναβαθμίσεων των εφαρμογών και υπηρεσιών σε θέματα ασφαλείας.

Από τα παραπάνω σημεία, συμπεραίνεται ότι τα θέματα ασφάλεια νεφοϋπολογιστικών συστημάτων έρχονται και προστίθενται στα θέματα ασφαλείας του IoT, δημιουργώντας ένα μεγαλύτερο προβληματισμό για την εφαρμογή περισσότερο ολοκληρωμένων μέτρων προστασίας.

Κεφάλαιο 3

Επισκόπηση στο σύγχρονο πλαίσιο προστασίας του IoT

3.1 Προτεινόμενο πλαίσιο προστασίας στο IoT

Το προτεινόμενο πλαίσιο στο Διαδίκτυο των Πραγμάτων έχει να κάνει με τις γενικότερες πολιτικές ασφαλείας, που πρέπει να ακολουθούνται ώστε να προστατεύονται οι διασυνδεδεμένες IoT συσκευές και κατ' επέκταση τα δεδομένα των χρηστών και η διακινούμενη πληροφορία.

Οι αρχιτεκτονικές IoT προσφέρουν τεράστιες δυνατότητες στην μετάδοση πληροφορίας και στην επικοινωνία των χρηστών. Αλλά την ίδια στιγμή, ως συνδυασμός ενσύρματων και ασύρματων δικτυακών κόμβων, οι αρχιτεκτονικές IoT κινδυνεύουν από τους κακόβουλους χρήστες. Έξυπνες συσκευές (π.χ. κινητά τηλέφωνα, ρολόγια, τηλεοράσεις, κλιματιστικά, ψυγεία, πλυντήρια, κ.α.), κάμερες και οποιαδήποτε άλλη συσκευή που συνδέεται στο Διαδίκτυο, είναι εκτεθειμένη σε οποιονδήποτε κακόβουλο χρήστη. Κακόβουλα εμπορικά προγράμματα μπορεί να εγκατασταθούν στις συσκευές IoT ή μια κυβερνητική ή μη κυβερνητική πηγή μπορεί να εισβάλλει στην λειτουργικότητα της αρχιτεκτονικής IoT ενός σπιτιού.

Το σημαντικό στοιχείο της δυσκολίας εφαρμογής μιας ενιαίας πολιτικής ασφαλείας στο IoT είναι ότι οι συμβατικές υπολογιστικές μηχανές (σταθεροί Η/Υ, laptops, servers, και κινητά τηλέφωνα) λειτουργούν υπό συγκεκριμένων διαχειριστικών και λειτουργικών εφαρμογών, με μια διευθυνσιοδότηση IPv4, και με συγκρινόμενες υπολογιστικές δυνατότητες. Για τον λόγο αυτό, μπορούν να βασιστούν σε ένα σταθερό

πλαίσιο πολιτικών ασφαλείας δικτύου, που περιλαμβάνει firewalls, προγράμματα προστασίας, κ.α.. Όμως, δεν συμβαίνει το ίδιο με το IoT, γιατί δεν αποτελεί ένα συμβατικό δίκτυο υπολογιστικών μηχανημάτων. Το IoT διαθέτει έναν μεγάλο αριθμό πρωτοκόλλων επικοινωνίας και τυποποίησης, που διαφοροποιούνται αναλόγως των διασυνδεδεμένων συσκευών, αυξάνοντας την πολυπλοκότητα σε μια σταθερή λύση ασφάλειας. Η προστασία του περιβάλλοντος IoT και η διαχείριση των θεμάτων ασφαλείας μπορούν να χωριστούν σε τρία επίπεδα, της συσκευής, του δικτύου και του Cloud (Εικόνα 10).

Εικόνα 10 . Περιγραφή σημαντικότερων σημείων ασφάλειας στο IoT.

Το σημαντικότερο θέμα στην ασφάλεια των IoT συστημάτων είναι η διαφύλαξη των δεδομένων που μεταδίδονται, ανταλλάσσονται και αποθηκεύονται. Κι αυτό, γιατί δεν υπάρχουν επαρκή πρωτόκολλα προστασίας επί των δεδομένων. Για παράδειγμα, υπάρχουν μεγάλοι προβληματισμοί στην χρήση των έξυπνων ρολογιών και άλλων φορητών συσκευών wearables, που συγκεντρώνουν δεδομένα ατομικής υγείας, τα οποία οι εμπορικές εταιρείες που ανήκουν τα λογισμικά υγείας, fitness, κλπ., μπορούν να συγκεντρώνουν αυτήν την πληροφορία, εγείροντας θέματα ιδιωτικότητας. Γι' αυτό και η εφαρμογή κρυπτογράφησης της πληροφορίας σε αυτές τις συσκευές στοχεύει στην προστασία των δεδομένων από άλλους χρήστες και στην διαχείριση του δικαιώματος προσπέλασης των ατομικών δεδομένων από άλλους.

Επειδή πολλές εταιρείες IT και τεχνολογίας, δεν ενημερώνουν τους πελάτες τους και πολλές φορές για να μειώσουν το κόστος δεν λαμβάνουν διαχειριστικά μέτρα προστασίας από malware, παρακάτω παρατίθενται συγκεντρωτικά πολιτικές και μέτρα ασφαλείας, που οφείλουν τόσο οι διαχειριστές και σχεδιαστές αρχιτεκτονικών IoT όσο και οι απλοί χρήστες των IoT συσκευών να εφαρμόζουν κατά το δυνατόν:

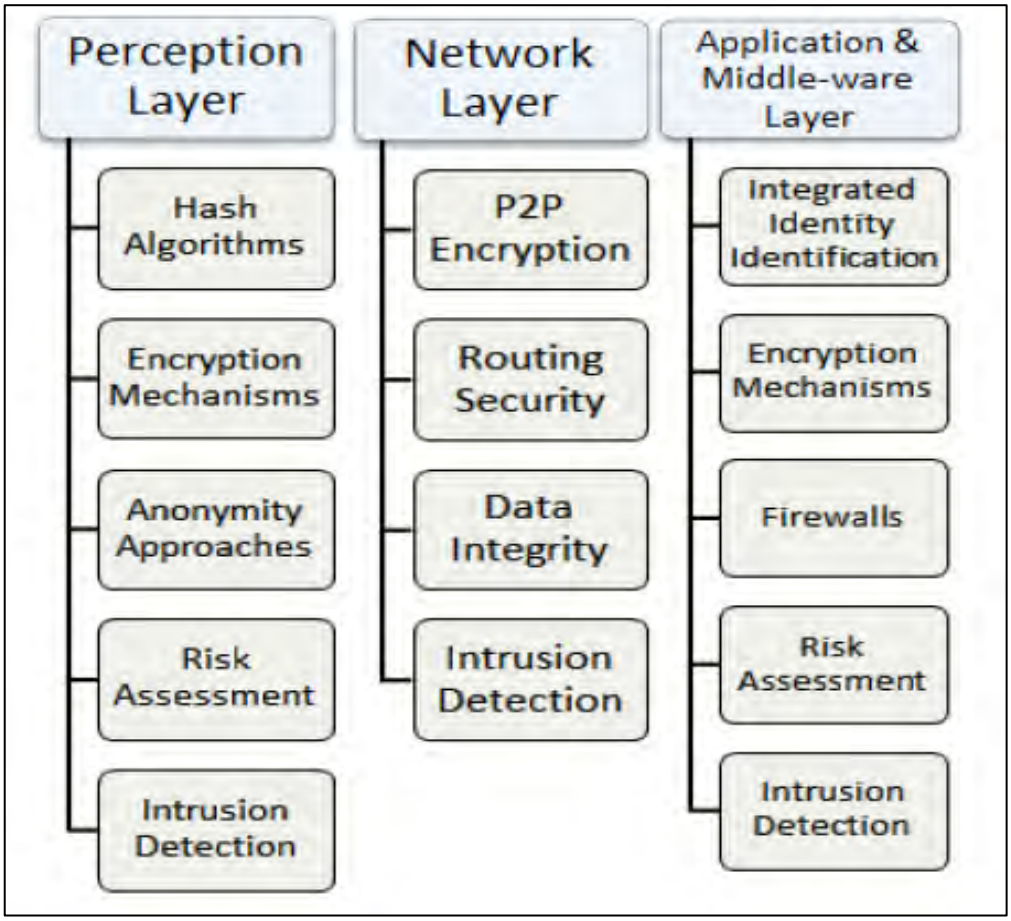
1. **Ενημέρωση:** Η ενημέρωση των χρηστών σε θέματα καλού χειρισμού των έξυπνων συσκευών, καθώς και η επιμόρφωση σε θέματα ασφαλείας στην Πληροφορική και στις Επικοινωνίες, αποτελεί σημαντικό σημείο στην εξελισσόμενη σημερινή ψηφιακή εποχή. Από την πλευρά των ειδικευμένων, ερευνητών, και εμπειρογνώμων της Πληροφορικής, των Δικτύων και της Τεχνολογίας, η ενημέρωση και η λήψη μέτρων προστασίας για την αντιμετώπιση κακόβουλου λογισμικού και κυβερνοεπιθέσεων, εξυπακούεται για την ασφάλεια οποιουδήποτε πληροφοριακού συστήματος και συστήματος επικοινωνίας.
2. **Ανάλυση Κινδύνου:** Οι οργανισμοί και οι επιχειρήσεις που συνήθως έχουν αρχιτεκτονικές IoT, είναι καλό να πραγματοποιούν μέσω εξειδικευμένων ατόμων με γνώσεις IoT security, ανάλυση κινδύνου και να μετρούν τον δείκτη ρίσκου ασφαλείας στις αρχιτεκτονικές τους, είτε πρόκειται για τα LAN δίκτυά τους που διασυνδέονται με έξυπνες συσκευές είτε με το Διαδίκτυο.

3. **Διαχείριση αυθεντικοποίησης:** Η διαχείριση των κωδικών εισόδου σε λογαριασμούς εφαρμογών και σε συσκευές IoT, τα λεγόμενα credentials, πρέπει να είναι ορθή, που δεν είναι άλλο παρά η πιστή τήρηση της πολιτικής της συχνής αλλαγής των credentials σε επίπεδο client. Τα credentials δεν πρέπει να είναι αδύναμα και συχνής ονοματολογίας, ενώ πρέπει να αλλάζονται σε τακτικό περιοδικό χρόνο. Προτείνονται πάντα στο ευρύτερο πλαίσιο της ασφάλειας, να είναι ένας συνδυασμός τουλάχιστον 8 χαρακτήρων, με εναλλαγές κεφαλαίων και μικρών γραμμάτων, αλφαριθμητικών και σημείων στίξης, ώστε να αποφεύγονται επιθέσεις τύπου brute-force.
4. **Ενημέρωση υλικο-λογισμικού:** Οι συσκευές IoT πρέπει να ενημερώνονται σε firmware. Οι ενημερωμένες εκδόσεις περιέχουν κώδικα αντιμετώπισης των νέων διαπιστευμένων ευπαθειών των συσκευών και λογισμικών.
5. **Firewalls:** Σε ένα απλό οικιακό δίκτυο, όλες οι συσκευές IoT συνδέονται στο Διαδίκτυο. Πρόκειται κυρίως για αισθητήρες χαμηλής ισχύος και έχουν περιορισμένους υπολογιστικούς πόρους. Ως εκ τούτου, δεν μπορούν να υποστηρίζουν ακριβή πρωτόκολλα κρυπτογράφησης. Για τον λόγο αυτό, είναι καλό να εγκαθίσταται σε ένα δίκτυο IoT ένα firewall, με σκοπό να προστατεύει τις διασυνδεδεμένες συσκευές. Επιπρόσθετα, πολλά routers έχουν ενσωματωμένα λογισμικά firewall, αλλά δεν είναι τόσο αποτελεσματικά όσο οι συσκευές firewall. Ο συνδυασμός όμως των routers με τα firewall δημιουργεί ένα εικονικό δίκτυο (VPN), με αποτέλεσμα ο χρήστης να μπορεί να συνδεθεί στο router του με μια υπηρεσία VPN, κρυπτογραφώντας την δικτυακή κίνηση [44].
6. **Ανανέωση των έξυπνων συσκευών:** Μπορεί η τεχνολογία να εξελίσσεται, αλλά την ίδια στιγμή εξελίσσονται και οι τρόποι επιθέσεων των κακόβουλων χρηστών. Ωστόσο, πρέπει να απομακρύνονται οι παλιές συσκευές και να αντικαθίστανται από νέας τεχνολογίας, γιατί οι πρώτες δεν βασίζονται στα νεώτερα πρωτόκολλα επικοινωνίας και διαθέτουν παλαιότερα, ξεχασμένα credentials σε επίπεδο εφαρμογών client και διαχείρισης. Σε ευρύτατα δίκτυα IoT η διαδικασία ανανέωσης έχει να κάνει με αυτό που ονομάζεται «lifecycle

management», δηλαδή την διαχείριση και τον έλεγχο απόδοσης και αντικατάστασης των συσκευών [45].

7. **Χρήση dynamic DNS και port forwarding:** Οι διαμορφώσεις αυτές επιτρέπουν την ασφαλέστερη είσοδο ενός χρήστη σε ένα οικιακό ή άλλο IoT δίκτυο απομακρυσμένα, καθώς χρησιμοποιείται τεχνική συνδυασμού ενός domain name με μια δυναμική IP διεύθυνση. Όλες οι άλλες πόρτες στις συσκευές IoT, και συγκεκριμένα στους routers, πρέπει να απενεργοποιούνται εφόσον δεν χρησιμοποιούνται [46].
8. **Χρήση περιήγησης Wireless Internet Service Provider (WISPr) και RADIUS server:** Οι τεχνικές λύσεις αυτές χρησιμοποιούνται από τους διαχειριστές των IoT περιβαλλόντων για την αυθεντικοποίηση και την εξουσιοδότηση των χρηστών σε ασύρματα δίκτυα WiFi που διασυνδέονται στο Διαδίκτυο [47].
9. **Κρυπτογράφηση των δεδομένων:** Οι σημαντικότεροι αλγόριθμοι κρυπτογράφησης είναι ο DES, ο TripleDES, ο AES, ο DSA και ο RSA. Μάλιστα, ο αλγόριθμος AES, μαζί με τον DSA και τον αλγόριθμο Rijndael, αποτελούν τον επίσημο συνδυασμό στην πολιτική χρήσης και ανταλλαγής κρυπτογραφημένης πληροφορίας στον δημόσιο τομέα των ΗΠΑ. Η χρήση του AES, μάλιστα, στην ασύρματη επικοινωνία διαφαίνεται αποτελεσματικότερη [48]. Επίσης, η κρυπτογράφηση της πληροφορίας στις αρχιτεκτονικές IoT και ειδικά στην νεφοϋπολογιστική του IoT, αποτελεί πολύ σημαντικό μέτρο προστασίας από κακόβουλες ενέργειες. Έτσι, πρέπει να εφαρμόζονται μέθοδοι κρυπτογράφησης των δεδομένων που ανακτώνται, μεταδίδονται και αποθηκεύονται στους Cloud Servers από IoT συσκευές [49].

Ένα περισσότερο συγκεντρωτικό και ολοκληρωμένο ίσως πλαίσιο ασφαλείας στο IoT προτάθηκε από τον Zhang *et al.* το 2013 [50],[51] (Εικόνα 11). Το συγκεκριμένο προτεινόμενο πλαίσιο ασφαλείας διαχωρίζεται ακολουθώντας την αρχιτεκτονική των συστημάτων IoT.



Εικόνα 11. Αρχιτεκτονική ασφαλείας συστημάτων IoT

Πιο αναλυτικά, στο Perception Layer που είναι το κατώτερο επίπεδο του IoT, οι πολιτικές και τα μέτρα προστασίας από κακόβουλους χρήστες αφορούν την αυθεντικοποίηση, την ιδιωτικότητα, την ανωνυμοποίηση και την διαχείριση κινδύνου των συσκευών (hardware). Η αυθεντικοποίηση και η ιδιωτικότητα επιτυγχάνεται με αλγορίθμους κρυπτογράφησης και ψηφιακών πιστοποιητικών. Η ανωνυμοποίηση των δεδομένων των χρηστών επιτυγχάνεται με την χρήση τεχνικών ανωνυμοποίησης (k-anonymization, κλπ.). Η διαχείριση κινδύνου επιτυγχάνεται με την αποτίμηση του

κινδύνου στο IoT περιβάλλον των συσκευών, η οποία αποτίμηση επιφέρει και την χάραξη στρατηγικών στην αντιμετώπιση των hackers σε φυσικό και hardware επίπεδο.

Στο Network Layer που περιλαμβάνει ενσύρματη και ασύρματη δικτύωση, οι πολιτικές και τα μέτρα προστασίας από hackers αφορούν, ομοίως, την αυθεντικοποίηση και την ιδιωτικότητα των δεδομένων, καθώς και την ασφάλεια στην δρομολόγηση των δεδομένων. Για την αυθεντικοποίηση πρέπει να χρησιμοποιούνται αλγόριθμοι κρυπτογράφησης point-to-point στους δικτυακούς κόμβους. Για την ασφάλεια στις δρομολογήσεις, πρέπει να χρησιμοποιούνται δικτυακές τεχνικές για την εξασφάλιση της δικτυακής κίνησης και την αναγνώριση πιθανών κινδύνων και λαθών.

Στο Application και Middleware Layer οι πολιτικές και τα μέτρα προστασίας από hackers αφορούν την αυθεντικοποίηση και την ιδιωτικότητα των δεδομένων σε τεχνολογίες Cloud και Virtualization. Συνδυάζουν τόσο λογισμικά antimalware όσο και υλικο-λογισμικά στην χρήση IPS/IDS τεχνολογιών.

3.2 Νέος Κανονισμός GDPR: τι σημαίνει για το IoT

Μια βιβλιογραφική έρευνα στις ΗΠΑ κατέδειξε κάποιους προβληματισμούς μεταξύ της ιδιωτικότητας της πληροφορίας και της αυθεντικοποίησης στο IoT. Οι προβληματισμοί αυτοί αφορούν τον σχεδιασμό και το κανονιστικό πλαίσιο υπηρεσιών αυθεντικοποίησης σε περιβάλλοντα IoT. Συγκεκριμένα, η ανασκόπηση κατέδειξε συσχέτιση των ταυτοτήτων χρηστών και των δεδομένων που παράγονται από περιβάλλοντα IoT, τα οποία δύναται να οδηγήσουν τους κακόβουλους χρήστες στην εκμετάλλευση του προφίλ και των προσωπικών δεδομένων του χρήστη. Επίσης, κατέδειξε τα κενά ασφαλείας που επιφέρουν την αποκάλυψη των ευαίσθητων πληροφοριών του χρήστη σε άλλους χρήστες IoT και εμπορικών οργανισμών – παρόχων IoT που διατηρούν δεδομένα των χρηστών, καθώς και τους περιορισμούς στην δυνατότητα του χρήστη IoT στην διαχείριση και στην παρακολούθηση της ιδιωτικότητάς του σε συσκευές και υπηρεσίες στο IoT, περιορισμοί οι οποίοι δύναται να διευκολύνουν παραβιάσεις της ιδιωτικότητας του χρήστη. Οι γενικότερες παραπάνω ενδείξεις, στοχεύουν στην ανάγκη ύπαρξης ενός νομικού και ρυθμιστικού πλαισίου

στους παρόχους συσκευών και υπηρεσιών IoT, και εν γένει στους φορείς αρχιτεκτονικών IoT, πάνω σε τέσσερις άξονες γύρω από την διακινούμενη πληροφορία και την υλικοτεχνική υποδομή των περιβαλλόντων IoT:

1. Στην διάκριση (discrimination)
2. Στην ιδιωτικότητα (privacy)
3. Στην ασφάλεια (security)
4. Στην συγκατάθεση (consent) [52].

Στο σημείο ακριβώς αυτό, έρχεται ο νέος Κανονισμός GDPR για να θέσει κάποια πλαίσια στην Ευρωπαϊκή Ένωση (ΕΕ), αλλά και σε οποιαδήποτε επιχειρηματική ή άλλου είδους δραστηριότητα σε παγκόσμιο επίπεδο που ενεργεί στην ΕΕ.

Ο νέος Κανονισμός Προστασίας Προσωπικών Δεδομένων (General Data Protection Regulation - GDPR) της ΕΕ εφαρμόστηκε από την 25η Μαΐου του 2018, κατόπιν πολλών περιστατικών επιθέσεων κακόβουλων χρηστών σε πληροφοριακά συστήματα της Ευρώπης και της ανάγκης ενός «roadmap» για την προστασία των δεδομένων ενός οργανισμού / επιχείρησης / ιδιωτικού φορέα, που αφορούν ευαίσθητες και προσωπικές πληροφορίες. Κάθε μία από τις προαναφερθέντες οντότητες πρέπει να διαθέτουν έναν Υπεύθυνο Επεξεργασίας Δεδομένων (Data Protection Officer – DPO), αλλά και άλλους ανθρώπους με ορισμένες αρμοδιότητες [53]. Ένα πολύ σημαντικό στοιχείο στον Κανονισμό GDPR είναι ότι στην προστασία των δεδομένων δεν εξετάζεται ο τρόπος που ακολουθείται για την καταγραφή, αποθήκευση και ασφάλεια των δεδομένων (ψηφιακά έγγραφα, ηχητικά δεδομένα και δεδομένα βιντεοσκόπησης, κ.α.) [54].

Ο Κανονισμός GDPR περιέχει πολλές προβλέψεις σχετικές με τους κινδύνους των σύγχρονων τεχνολογιών. Ωστόσο, το αυστηρό κανονιστικό πλαίσιο ίσως είναι αναποτελεσματικό για την διασφάλιση των θεμάτων ασφαλείας της ιδιωτικότητας δεδομένων των χρηστών στα IoT συστήματα. Επιπρόσθετα, ίσως είναι αναποτελεσματικό στην ανάληψη υποχρεώσεων των εμπορικών εταιριών που

υποστηρίζουν τεχνολογίες IoT και διατηρούν δεδομένα. Γενικότερα όμως, στο πλαίσιο των τεχνολογιών διαπίστευσης και ταυτοποίησης του χρήστη στις τεχνολογίες IoT, ο GDPR παρέχει ένα ικανοποιητικό οδηγό για τη νομική προσαρμογή όλων των εμπλεκομένων φορέων που διαχειρίζονται προσωπικά δεδομένα, ανεξαρτήτως χώρας προέλευσης. Όσο οι τεχνολογίες IoT συλλέγουν, αποθηκεύουν και διαμοιράζουν πληροφορίες, ειδικά όσον αφορά προσωπικά δεδομένα, ο Κανονισμός GDPR είναι υποχρεωτικό να αξιοποιηθεί ως εκάστοτε κυβερνητική πολιτική για τον σχεδιασμό και εφαρμογή IoT αρχιτεκτονικών.

Κάθε οντότητα (οργανισμός / επιχείρηση / δημόσιος ή ιδιωτικός φορέας, κλπ.) πρέπει να συμμορφώνεται με τον Κανονισμό, να είναι δηλαδή «GDPR compliant». Οπότε, το ίδιο ισχύει και για τους παρόχους, εμπόρους, επιχειρήσεις, και οποιαδήποτε οντότητα των IoT συστημάτων. Ο Κανονισμός έχει απλωθεί και πέραν της ΕΕ, καθώς πολλές εταιρείες IoT είναι πολυεθνικής ιδιοκτησίας και συνεργασίας. Οι κρίσιμες αναφορές στην σχετική θεματολογία περί ιδιωτικότητας, αυθεντικοποίησης και ταυτοποίησης στα συστήματα IoT, περιλαμβάνουν μια σειρά από Άρθρα και αναφορικά κείμενα στον Κανονισμό. Στοχεύουν δε, στην πλήρη εναρμόνιση όλων των οντοτήτων – φορέων τεχνολογίας IoT σε έξυπνες συσκευές, κινητό ενεργό εξοπλισμό, εξοπλισμό ασύρματης τεχνολογίας, αισθητήρων, υπηρεσιών IoT Cloud, κλπ. Ο GDPR κάνει ιδιαίτερη μνεία στα Άρθρα του σχετικά με:

- Την διαφάνεια, την αποθήκευση, την πρόσβαση και την επεξεργασία της διακινούμενης πληροφορίας.
- Τις διαδικασίες ενημέρωσης και συγκατάθεσης των χρηστών.
- Τις αυτόματες διαδικασίες σε συστήματα υποστήριξης αποφάσεων και διαχείρισης προφίλ χρηστών.
- Τις ασφαλείς διαδικασίες σχεδιασμού συσκευών και ηλεκτρονικών υπηρεσιών, τύπου «privacy by design» και «privacy by default».
- Τις διαδικασίες εκτίμησης της προστασίας των δεδομένων (Data Protection Impact Assessment – DPIA).
- Τις πολιτικές προστασίας από κυβερνοεπιθέσεις.

- Τις πολιτικές καταγραφής και εκτίμησης της απώλειας ή υποκλοπής ή τροποποίησης δεδομένων.
- Τις πολιτικές καταγραφής της ροής διακίνησης και καταχώρησης της πληροφορίας.

Η επιρροή του GDPR, κατόπιν των ανωτέρω, είναι εμφανής στους διαχειριστές και παρόχους IoT τεχνολογίας, καθώς πρέπει, οπωσδήποτε και κατ' ελάχιστον, να συμμορφώνονται σε διαδικασίες ενημέρωσης των χρηστών IoT, λόγω της έλλειψης τεχνικά τυποποιημένων μεθόδων προστασίας των δεδομένων. Οι δηλώσεις DPIA από τους IoT παρόχους λαμβάνονται ως αναξιόπιστες με βάση την υποκειμενικότητα της αξίας των προσωπικών δεδομένων που παράγονται και διακινούνται δια μέσου των IoT συσκευών και υπηρεσιών.

Εν τέλει, ο νέος Κανονισμός GDPR έχει άμεση επιρροή στο IoT. Οι αρχές συμμόρφωσης και προσαρμογής των IT φυσικών και νομικών προσώπων, γύρω από την διαφάνεια και την προστασία της πληροφορίας σε σχέση με τις δυνατότητες και την εφαρμογή αυτών στο IoT, συνοψίζονται ως εξής [55]:

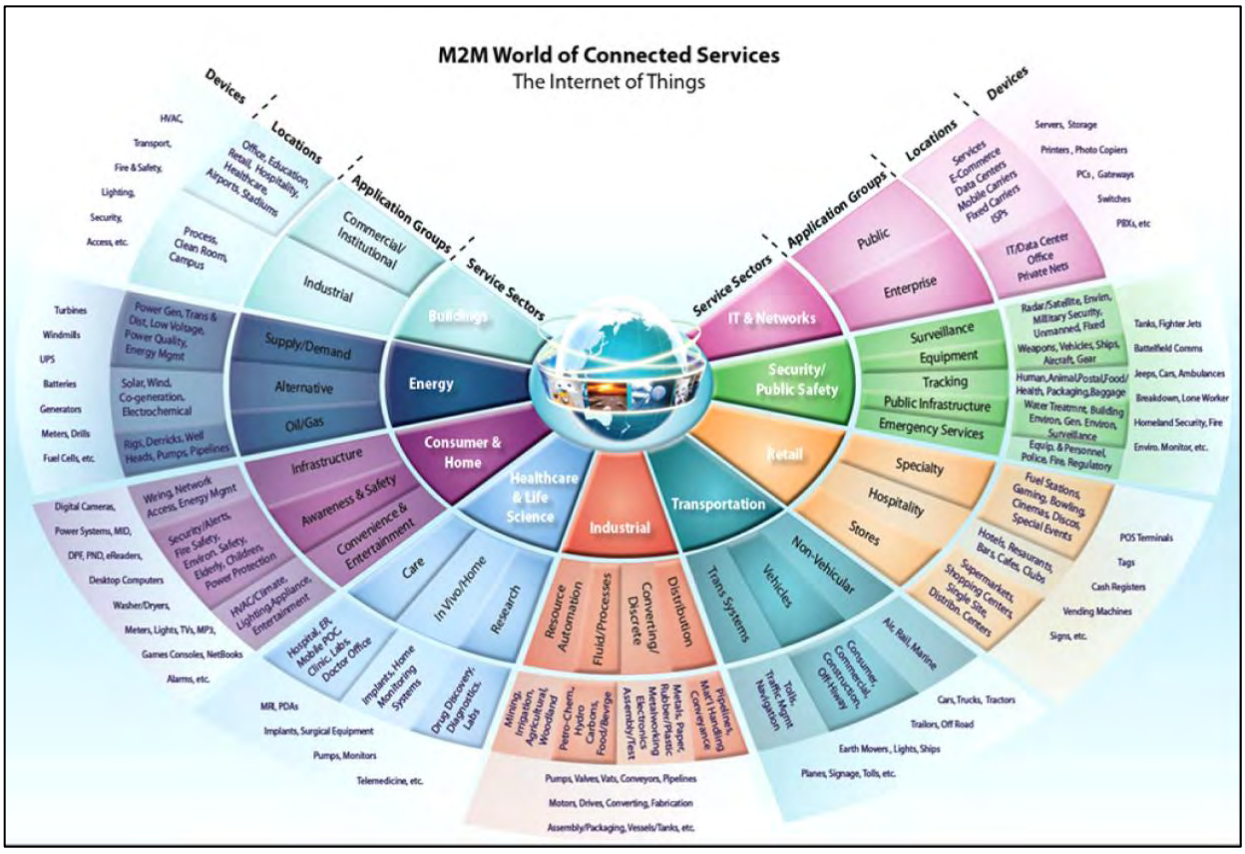
1. Αρχή της διαφάνειας και σύννομες διαδικασίες προστασίας των προσωπικών δεδομένων των χρηστών από οποιαδήποτε οντότητα διαχείρισης δεδομένων (data controller): απαιτούνται ενέργειες στο IoT και εφαρμόζεται δύσκολα.
2. Αρχή του περιορισμού στην συλλογή και εκμετάλλευση δεδομένων από τους data controllers: απαιτούνται ενέργειες στο IoT και εφαρμόζεται δύσκολα.
3. Αρχή της διατήρηση της ακρίβειας και των πληροφοριών: απαιτούνται ενέργειες στο IoT και εφαρμόζεται δύσκολα.
4. Αρχή του περιορισμού του χώρου αποθήκευσης πληροφορίας: εφαρμόσιμο στο IoT, αλλά έρχεται σε σύγκρουση με τα συμφέροντα των διαφόρων IT εταιρειών.
5. Αρχή της ακεραιότητας και της εμπιστευτικότητας των δεδομένων: απαιτούνται ενέργειες στο IoT (device identifiers, apps identifiers, cookies, κ.α.), αλλά ειδικά για τα ασύρματα LAN δίκτυα και τις τεχνολογίες RFID καρτών είναι δύσκολα εφαρμόσιμη, για την προστασία αυτών από κυβερνοεπιθέσεις.

6. Αρχής της ευθύνης καταγραφής της ροής της πληροφορίας: οι DPIAs είναι δύσκολα εφαρμόσιμες στο IoT, αλλά απαραίτητες και υποχρεωτικές.

Κεφάλαιο 4

Συμπεράσματα

Η IoT τεχνολογία είναι παρόν και το μέλλον της ανήκει. Μέχρι το 2050 οι «έξυπνες» πόλεις (smart cities) θα είναι γεγονός, με περισσότερα από 50 δισεκατομμύρια διασυνδεδεμένες συσκευές, φαινόμενο γνωστό ως “Machine to Machine (M2M) connections» (Εικόνα 12).



Εικόνα 12. Machine to Machine διασυνδέσεις στο IoT.

Το IoT επηρεάζει όλους τους τομείς της σύγχρονης κοινωνίας, όπως την Ενέργεια, την Υγεία, τις Μεταφορές, την Βιομηχανία, την Δημόσια Ασφάλεια, την Τραπεζική κλπ. Τίποτα δεν φαίνεται να στέκεται εμπόδιο στην ανάπτυξη του IoT παρά μόνο τα ζητήματα της ασφάλειας. Ήδη, wearables, έξυπνα αυτοκίνητα, IoT κάμερες και smart devices, κ.α., κατακλύζουν τον κόσμο. Επιπροσθέτως, η μείωση των τιμών σε κόστος συσκευών, δίσκων αποθήκευσης, ανακατασκευασμένων (refurbished) ενεργών εξοπλισμών, η μείωση του κόστους ανάπτυξης εφαρμογών, καθώς και η έλευση νέων καινοτόμων τεχνολογιών, όπως η ανάπτυξη δικτύων οπτικών ινών, δικτύων τεχνολογίας 5G, κλπ., ανοίγουν διάπλατα το δρόμο για την επέκταση των IoT τεχνολογιών και της διασύνδεσης τόσο μεταξύ τους όσο και με το Διαδίκτυο.

Η τεχνολογία διαπίστευσης και προστασίας της πληροφορίας στο IoT έχει δημιουργήσει πολλά ερωτήματα και ανησυχίες. Ωστόσο, μέχρι στιγμής έχουν υλοποιηθεί και συνεχώς αναπτύσσονται τεχνολογίες, πολιτικές και θεσμικά κείμενα, που στοχεύουν στην αυξανόμενη διασφάλιση της επικοινωνίας, την διασφάλιση των προσωπικών και ευαίσθητων δεδομένων των χρηστών, και την αποτροπή οποιασδήποτε κακόβουλης ενέργειας. Τα συστήματα IoT δημιουργούν και συντηρούν τεράστιες ποσότητες ψηφιακών δεδομένων, που παράγονται από διαφορετικές πηγές και διακινούνται σε διαφορετικές δικτυακές διασυνδεδεμένες συσκευές. Οι χαμηλές ενεργειακά συσκευές IoT και η έλλειψη δεσμεύσεων και ελεγκτικών μηχανισμών σε IoT εταιρείες και κρατικούς φορείς αντίστοιχα, καταστεί τα περιβάλλοντα IoT ευάλωτα σε επιθέσεις κακόβουλων χρηστών. Ο Κανονισμός GDPR στοχεύει στις περαιτέρω ενέργειες νομοθεσίας και δημιουργίας ελεγκτικών μηχανισμών σε εθνικό επίπεδο, καθώς και σε περαιτέρω τεχνικές ενέργειες από τους ιδιωτικούς και δημόσιους φορείς IT τεχνολογίας, με σκοπό να καλυφθούν όσο το δυνατόν τα ζητήματα ασφαλείας δεδομένων, χωρίς να παρακωλύονται οι υπηρεσίες IoT.

Παρόλες τις διαπιστώσεις και τα προτεινόμενα μέτρα ασφαλείας γύρω από το IoT, συνεχώς λαμβάνονται νέα μέτρα και δημιουργούνται νέα λογισμικά για την αντιμετώπιση των ευπαθειών των συσκευών και λογισμικών IoT. Ωστόσο, για τον περιορισμό των κακόβουλων επιθέσεων και την εκμετάλλευση αδυναμιών στα διάφορα

συστήματα, απαιτείται η ευαισθητοποίηση του κόσμου στα ζητήματα της Ασφάλειας των Πληροφοριακών Συστημάτων εν γένει. Στην χώρα μας και διεθνώς, διεξάγονται μαθήματα Υπολογιστών, Πληροφορικής, Προγραμματισμού και Διαδικτύου. Οι διεπαφές στις ηλεκτρονικές συσκευές και η διαδικτύωση με τον Παγκόσμιο Ιστό, απαιτεί και την κατ' ελάχιστον εκπαίδευση στην ΑΠΣ και στα ατομικά και συλλογικά μέτρα προστασίας.

Βιβλιογραφικές & Διαδικτυακές Πηγές

[1] Gubbi et al. (2013) Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Generation Computer Systems, pp.1645–1660.

[2] Towards a definition of the Internet of Things - Revision 1 - published on May 2015, Available from *https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf*, Last accessed Mar '19.

[3] https://el.wikipedia.org/wiki/Διαδίκτυο_των_πραγμάτων, Last accessed Apr '19

[4] https://www.tutorialspoint.com/internet_of_things/index.htm, Last accessed Apr '19

[5] Dorsemaine B., et al., IEEE 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies

[6] Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures

[7] Atzori L. et al.. (2012) The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization. Computer Networks, volume 56:3594-3608.

[8] Zhang W. and Qu B. (2013) Security architecture of the Internet of Things oriented to perceptual layer. Int J Comput, Consum Control (IJ3C.volume 2(2):37–45.

[9] Leo M. et al.. A federated architecture approach for Internet of Things security. Euro Med Telco Conference (EMTC). 2014.

[10] http://jin.ece.ufl.edu/papers/HASS2018_IoT_Survey.pdf, Last accessed Apr '19

[11] http://blog.isecurion.com/2017/05/11/iot-communication-protocols/, Last accessed Apr '19

[12] https://www.slideshare.net/AbdullahAlfadhly/introduction-to-iot-architectures-and-protocols, Last accessed Apr ‘19

[13] https://iot-analytics.com/10-internet-of-things-applications/, Last accessed, Apr ’19

[14] https://aioti.eu/wp-content/uploads/2017/03/AIOTIWG01Report2015-Applications.pdf, Last accessed, Apr ’19

[15] Πάγκαλου Γ., Μαυρίδη Ι. (2002) Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων. Θεσσαλονίκη: Εκδόσεις Ανικούλα.

[16] Κάτσικα Σ., Γκρίτζαλη Δ., Γκρίτζαλη Σ. (2004) Ασφάλεια Πληροφοριακών Συστημάτων. Αθήνα: Εκδόσεις Νέων Τεχνολογιών.

[17] https://en.wikipedia.org/wiki/Cyberspace, Last accessed, Apr ’19

[18] https://en.wikipedia.org/wiki/Privacy, Last accessed, Apr ’19

[19] Nan Y, Yang M, Yang Z, Zhou S, Gu G, Wang X (2015) UIPicker: user-input privacy identification in mobile applications. In: USENIX Security Symposium, pp 993–1008.

[20] Fernandes E, Jung J, Prakash A (2016) Security analysis of emerging smart home applications. In: 2016 IEEE Symposium on Security and Privacy (SP). IEEE, pp 636–654.

[21] Fernandes E, Paupore J, Rahmati A, Simionato D, Conti M, Prakash A (2016). In: USENIX Security Symposium, pp 531–548.

[22] https://en.wikipedia.org/wiki/Phishing, Last accessed, Apr ’19

[23] Thakur BS, Chaudhary S (2013) Content sniffing attack detection in client and server side: a survey. Int J Advan Comput Res 3(2):7.

[24] Alqassem I, Svetinovic D (2014) A taxonomy of security and privacy requirements for the Internet of Things (IoT). In: 2014 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). IEEE, pp 1244–1248.

[25] Gruschka N, Jensen M (2010) Attack surfaces: a taxonomy for attacks on cloud services. In: 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD). IEEE, pp 276–279.

[26] Jensen M, Schwenk J, Gruschka N, Iacono LL (2009) On technical security issues in cloud computing. In: 2009 IEEE International Conference on Cloud Computing. CLOUD'09. IEEE, pp 109–116.

[27] Dorai R, Kannan V (2011) SQL injection—database attack revolution and prevention. J Int'l Com L & Tech 6:224.

[28] Wang K. and Hou Y. (2016) Detection method of SQL injection attack in cloud computing environment. IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Xi'an, pp.487-493. DOI:10.1109/IMCEC.2016.7867260.

[29] Sastry AS, Sulthana S, Vagdevi S (2013) Security threats in wireless sensor networks in each layer. Int J Advan Netw Appl 4(4):1657.

[30] https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/, Last accessed May '19

[31] Wang, Liang; Kangasharju, Jussi (2012) Real-world sybil attacks in BitTorrent mainline DHT. 2012 IEEE Global Communications Conference (GLOBECOM). pp. 826–32.

[32] Wang, Liang; Kangasharju, Jussi (2013). Measuring large-scale distributed systems: case of BitTorrent Mainline DHT. IEEE P2P 2013 Proceedings. pp. 1–10.

[33] Padmavathi DG, Shanmugapriya M et al (2009) A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv:0909.0576.

[34] Cho J-S, Yeo S-S, Kim SK (2011) Securing against brute-force attack: a hash-based RFID mutual authentication protocol using a secret value. Comput Commun v.34(3), pp.391–397.

[35] https://www.veracode.com/security/man-middle-attack, Last accessed May '19

[36] Kasper T. et al. (2011) Wireless security threats: Eavesdropping and detecting of active RFIDs and remote controls in the wild. 19th International Conference on Software, Telecommunications and Computer Networks, Split, pp.1-6.

[37] Jha RK and Dalal UD (2010) Performance comparison of Intelligent Jamming in RF (Physical) Layer with WLAN Ethernet Router and WLAN Ethernet Bridge. 2010 ITU-T Kleidoscope: Beyond the Internet? – Innovations for Future Networks and Services, Pune, pp.1-6.

[38] https://en.m.wikipedia.org/wiki/Eavesdropping, Last accessed May ’19

[39] Mitrokotsa A, Rieback MR, Tanenbaum AS (2010) Classification of RFID attacks. Gen 15693:14443.

[40] https://journals.sagepub.com/doi/full/10.1080/15501320600642718, Last accessed May ’19

[41] Zhou J. et al (2017) Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures, and Future Directions. IEEE Communications Magazine. DOI:10.1109/MCOM.2017.1600363CM.

[42] Bhattasali, T., Chaki, R. and Chaki, N. (2013) Secure and trusted cloud of things. In: India Conference (INDICON), 2013 Annual IEEE. IEEE, pp. 1–6.

[43] Stergiou C. et al (2016) Secure integration of IoT and Cloud Computing. Future Generation Computer Systems. http://dx.doi.org/10.1016/j.future.2016.11.031

[44] Gupta N. et al. (2017) A Firewall for Internet of Things. 2017 9th International Conference on Communication Systems and Networks (COMSNETS).

[45] https://medium.com/iotforall/a-beginners-guide-to-securing-your-iot-devices-16dfc0122a17, Last accessed June ’19

[46] https://stevessmarthomeguide.com/dynamic-dns/, Last accessed June ’19

[47] Mahmoud R. et al. (2015) Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures. 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015)

[48] Sujithra M. et al. (2015) Mobile Device Data Security: A Cryptographic Approach by Outsourcing Mobile Data to Cloud. Procedia Computer Science. vol.47, pp.480-485.

[49] https://www.iotforall.com/future-iot-encryption, Last accessed June ’19

[50] Zhang W. and Qu B. (2013) Security Architecture of the Internet of Things Oriented to Perceptual Layer. International Journal on Computer, Consumer and Control (IJ3C).vol.2;2.

[51] Farooq MU et al. (2015) A Critical Analysis on the Security Concerns of Internet of Things (IoT). International Journal of Computer Applications.vol.111;7.

[52] https://texaslawreview.org, Last accessed June ’19

[53] https://eugdpr.org/, Last accessed June ’19

[54] Watson D. and Millerick R. (2019) GDPR and employee data protection: Cyber security data example. Cyber Security. vol;2(1), pp.23-30.

[55] Sandra Wachter (2018): The GDPR and the Internet of Things: a three-step transparency model, Law, Innovation and Technology, DOI: 10.1080/17579961.2018.1527479.